

FIG. 1

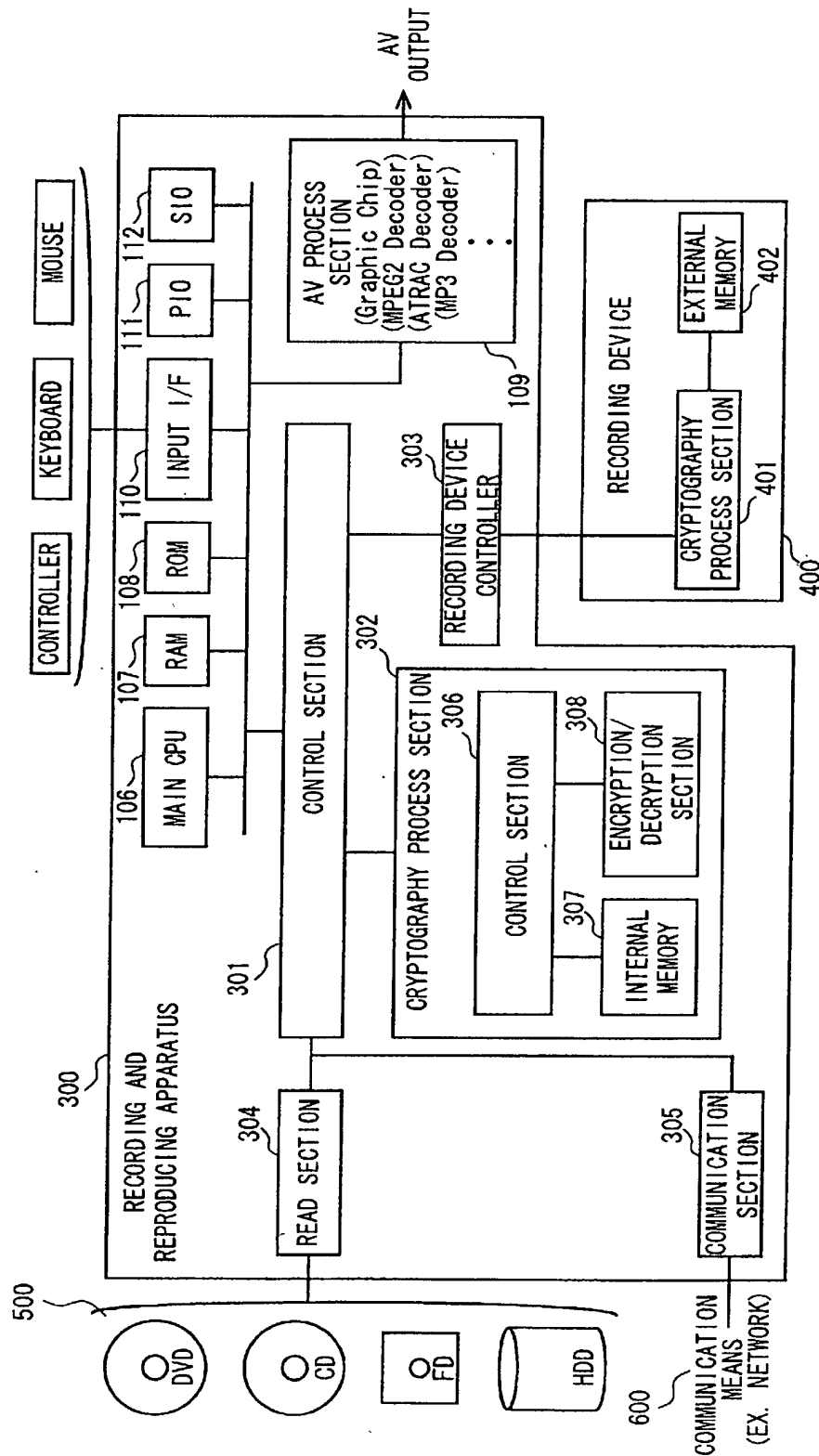


FIG. 2

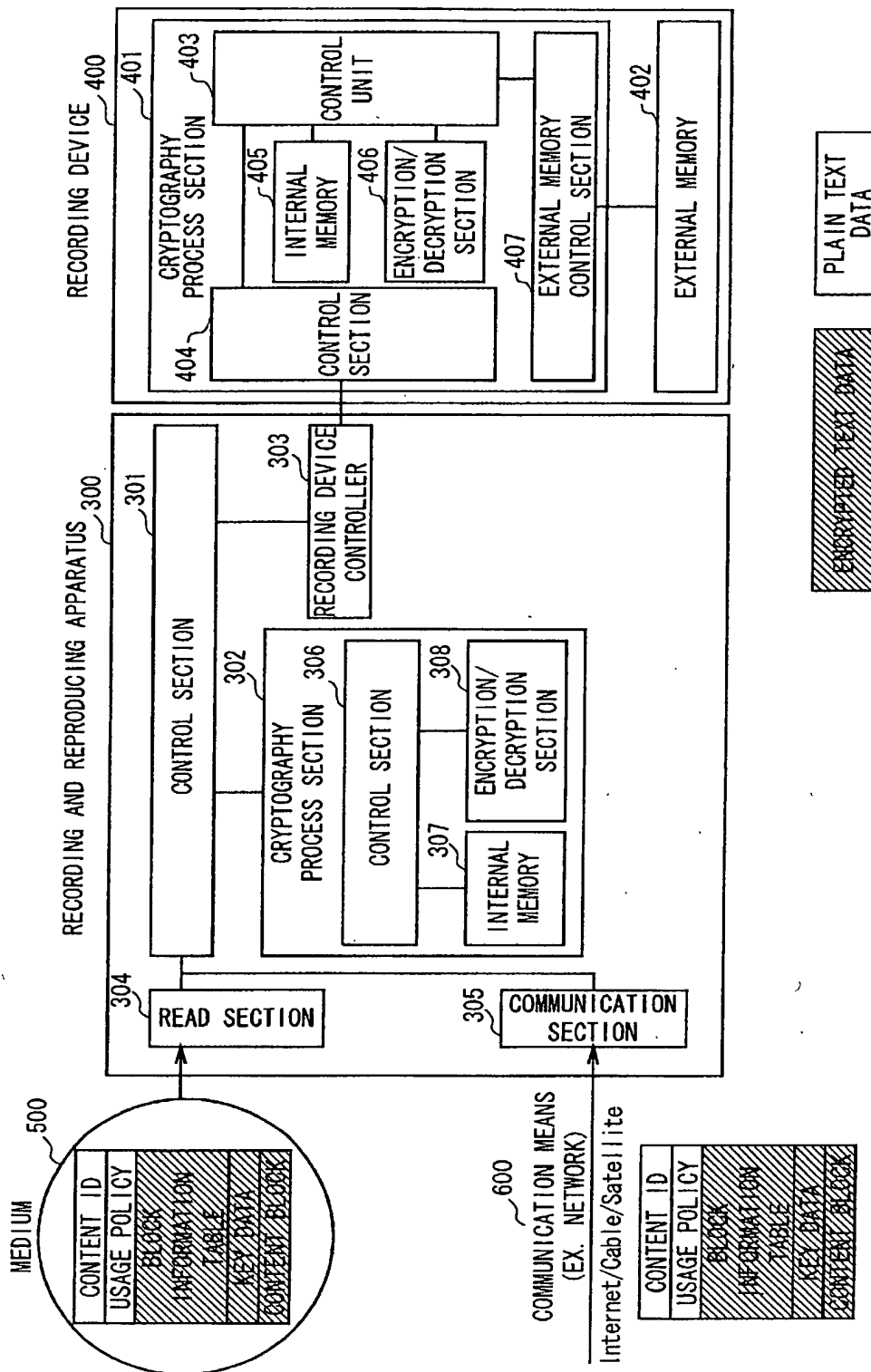
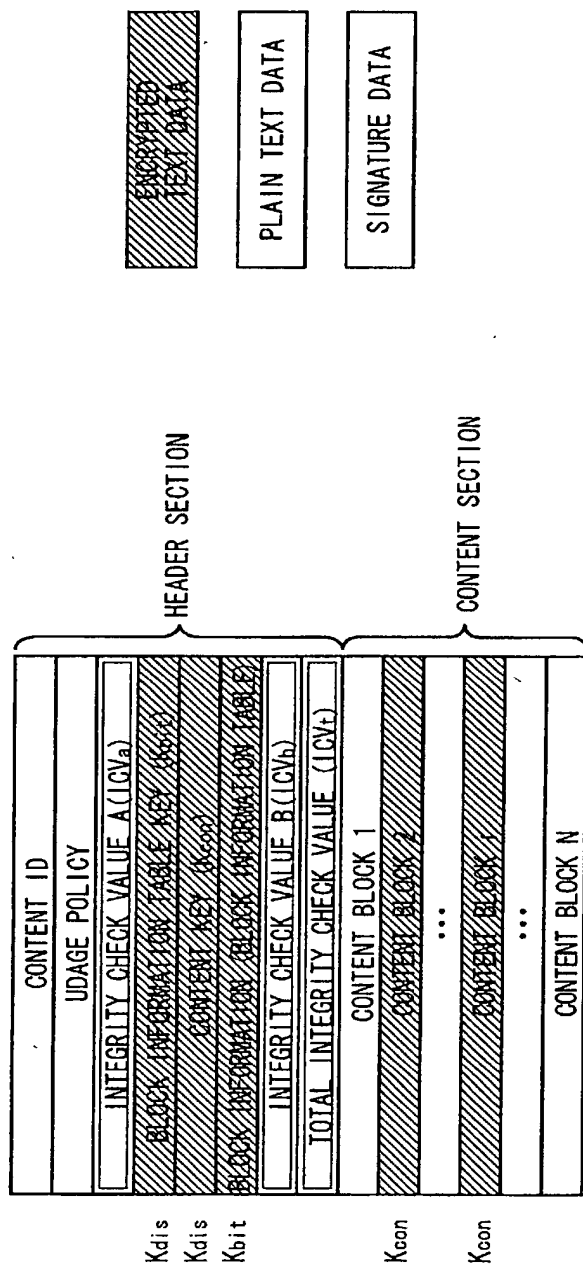


FIG. 3



DATA FORMAT ON MEDIUM AND COMMUNICATION PATH

FIG. 4

HEADER LENGTH
CONTENT LENGTH
FORMAT VERSION
FORMAT TYPE
CONTENT TYPE
OPERATION PRIORITY
LOCALIZATION FIELD
COPY PERMISSION
MOVE PERMISSION
ENCRYPTION ALGORITHM
ENCRYPTION MODE
INTEGRITY CHECK METHOD

USAGE POLICY

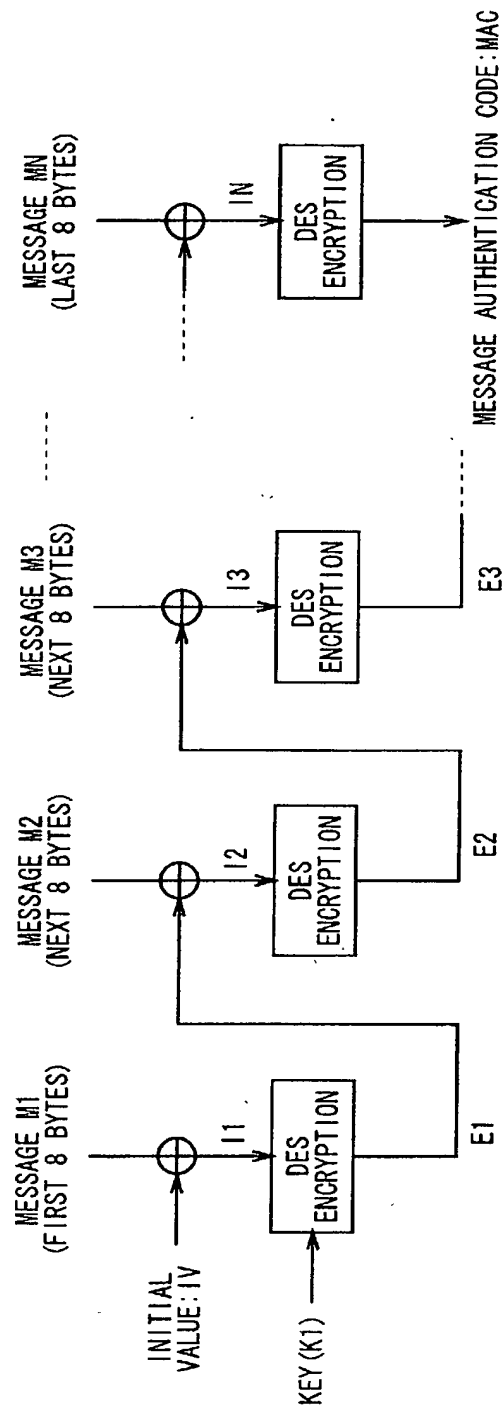
FIG. 5

Kbit

BLOCK 1	BLOCK NUMBER
	BLOCK LENGTH
	ENCRYPTION FLAG
	FLAG TO BE VERIFIED (ICV FLAG)
	ICV1
BLOCK N	.
	.
	.
	.
	.
BLOCK N	BLOCK LENGTH
	ENCRYPTION FLAG
	ICV FLAG
	CONTENT INTEGRITY CHECK VALUE (ICVN)

BLOCK INFORMATION TABLE

FIG. 6



⊕: EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FIG. 7

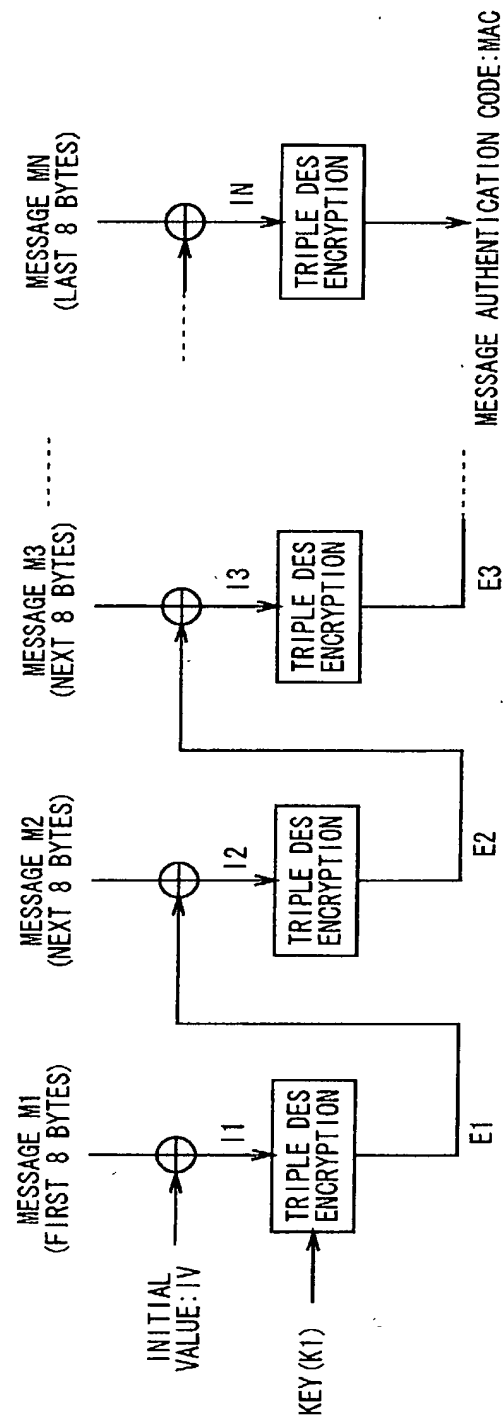


FIG. 8



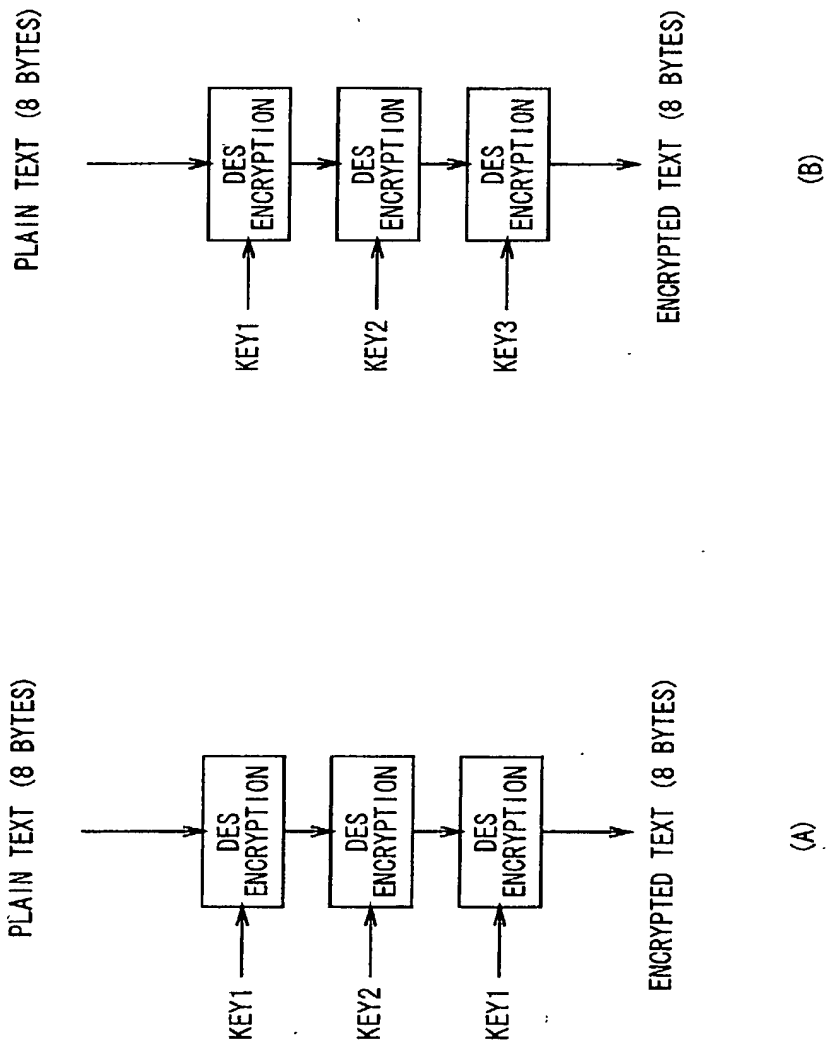


FIG. 9



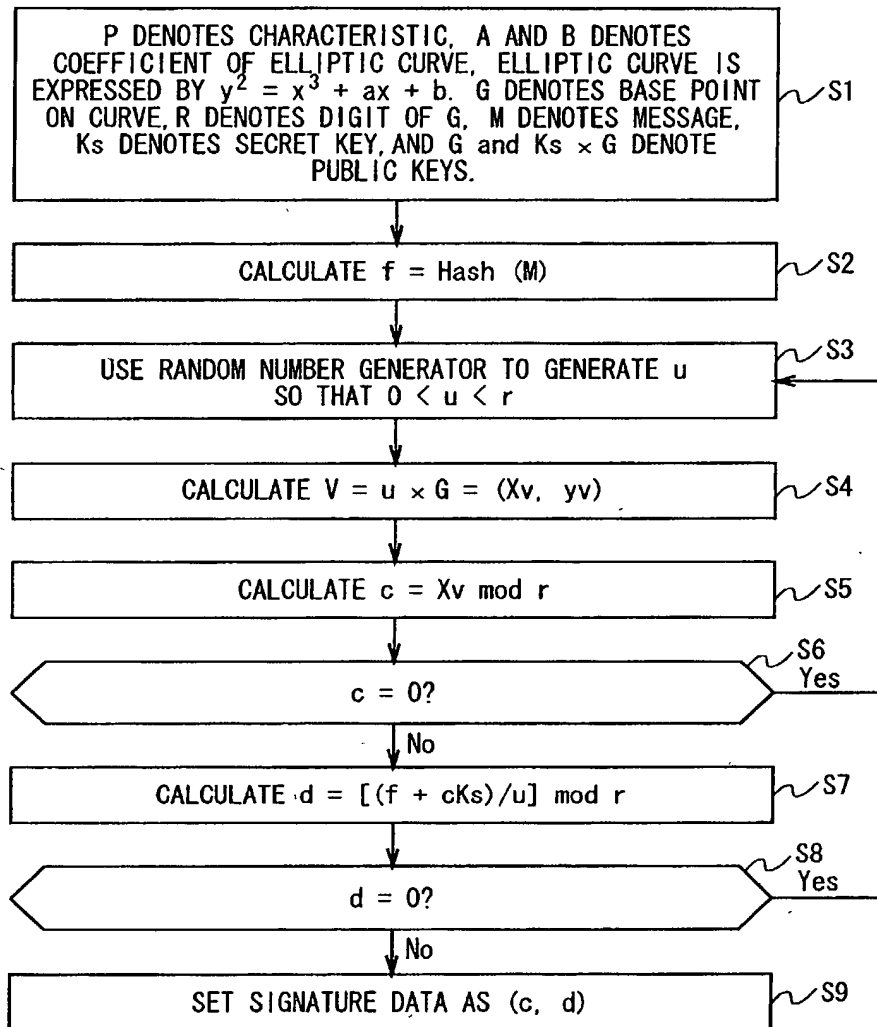
SIGNATURE GENERATIONGENERATION OF SIGNATURE (IEEE P1363/D3)

FIG. 11

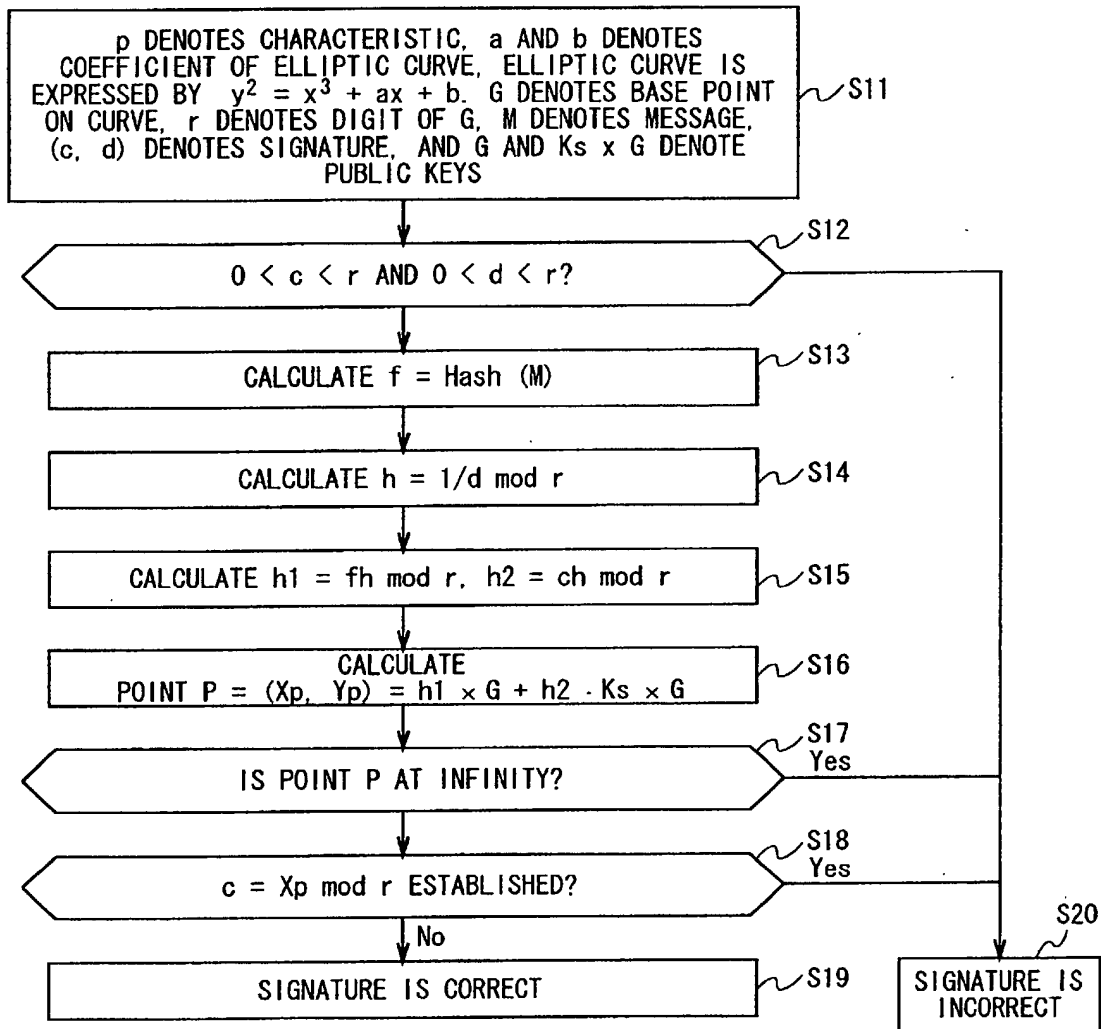
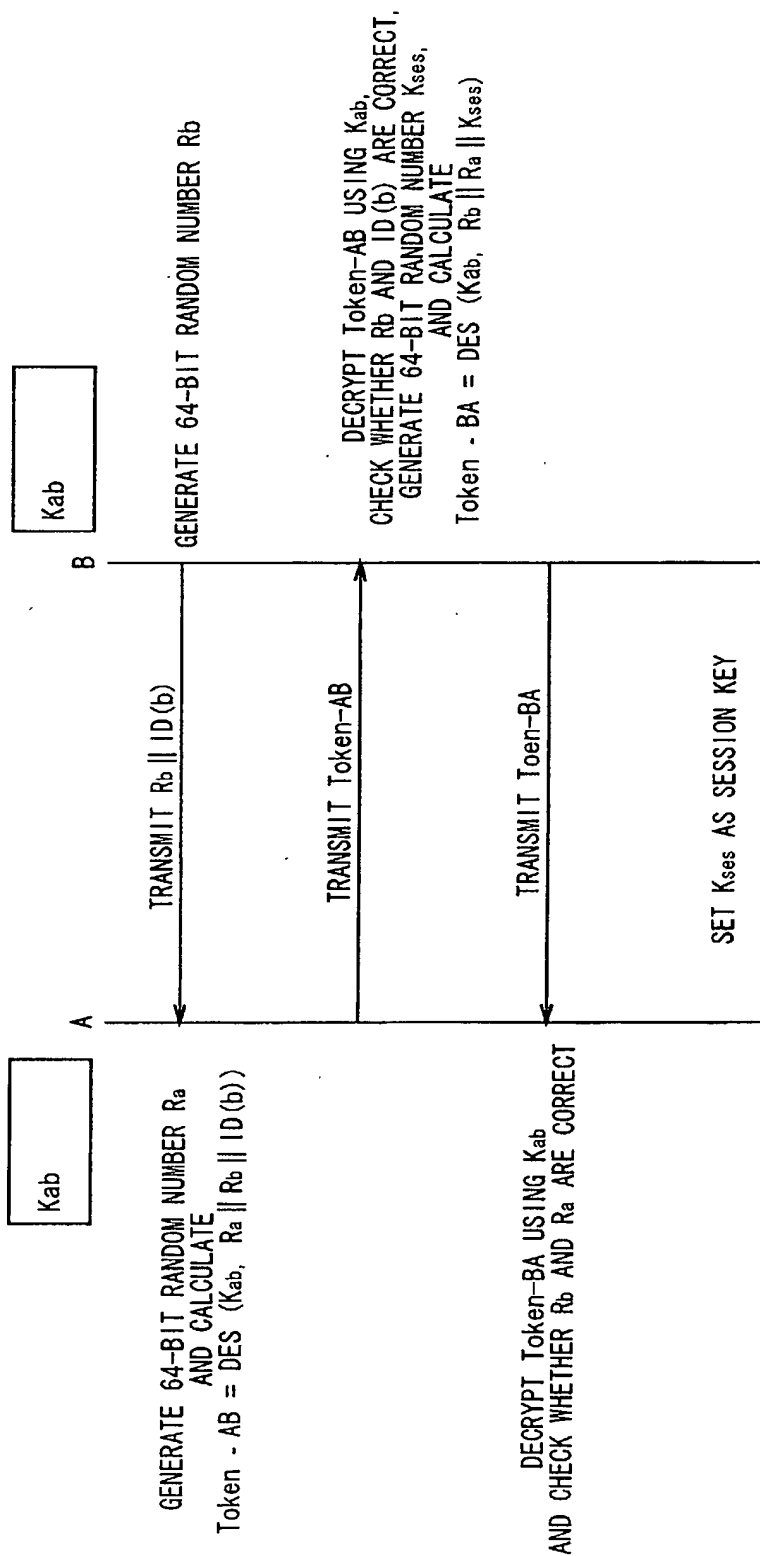
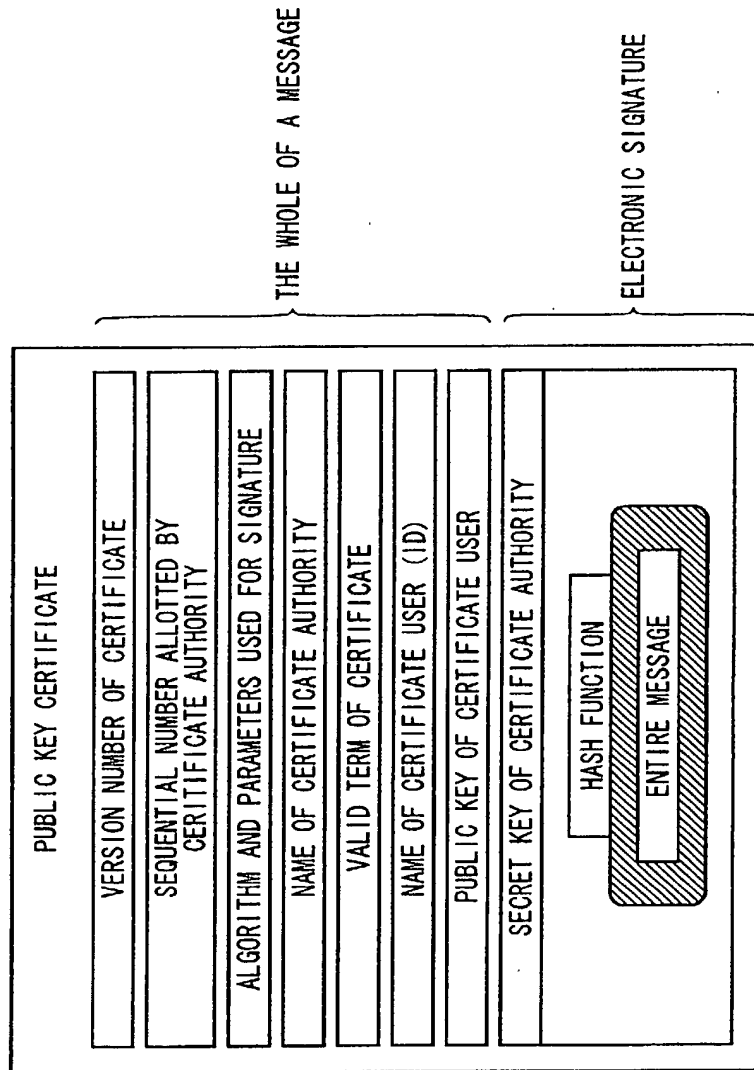
SIGNATURE VERIFICATIONSIGNATURE VERIFICATION(IEEE P1363/D3)

FIG. 12



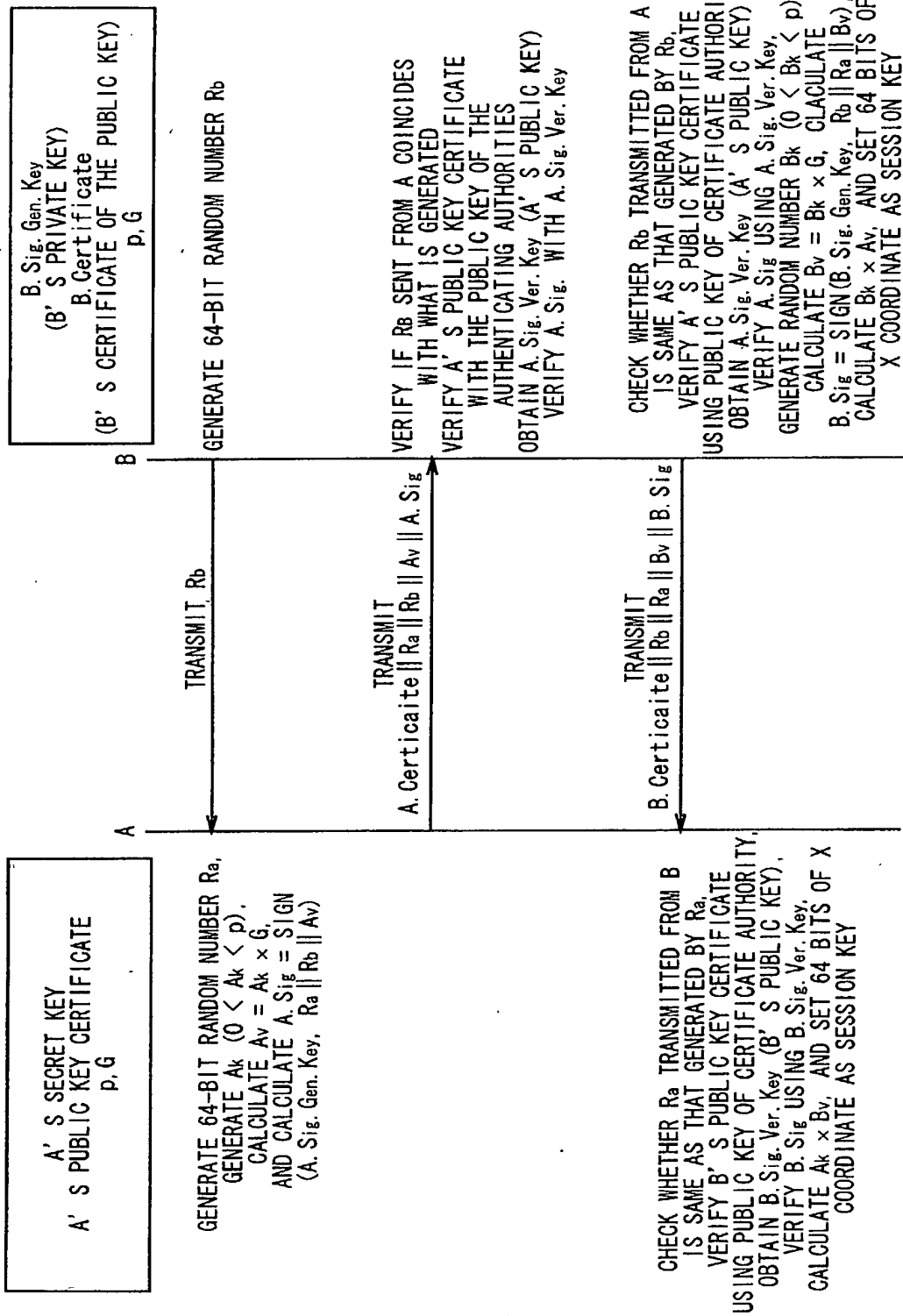
SECRET 02146600



PUBLIC KEY CERTIFICATE

FIG. 14

SECRET 0274660



ISO/IEC 9798-3 MUTUAL AUTHENTICATION AND KEY SHARING METHOD USING SYMMETRICAL KEY CRYPTOGRAPHY TECHNIQUE

FIG. 15

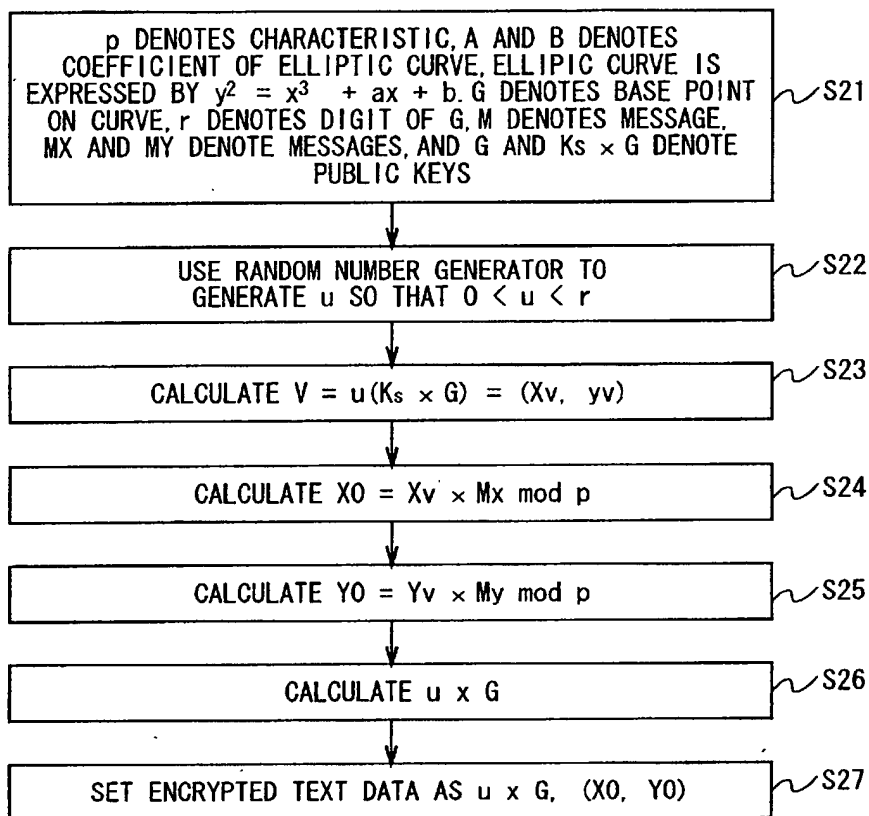
ENCRYPTIONENCRYPTION USING ELLIPTIC CURVE CRYPTOGRAPHY (MENEZES-VANSTONE)

FIG. 16



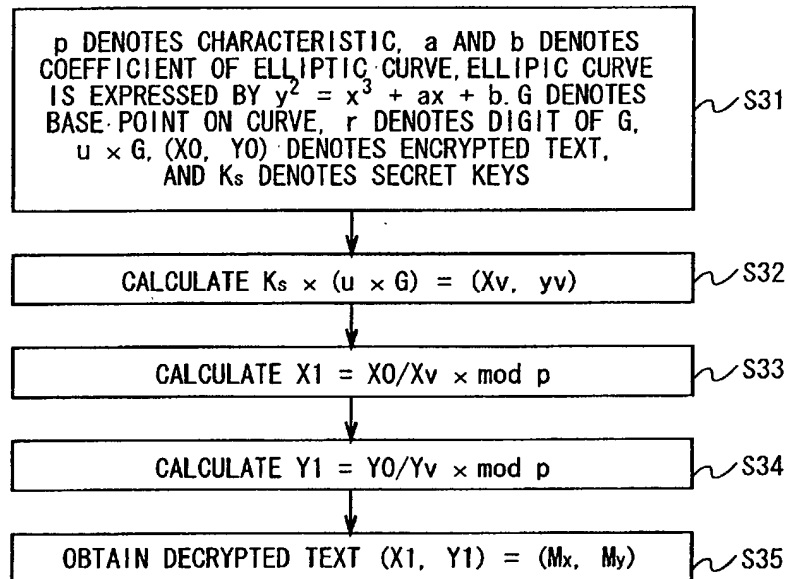
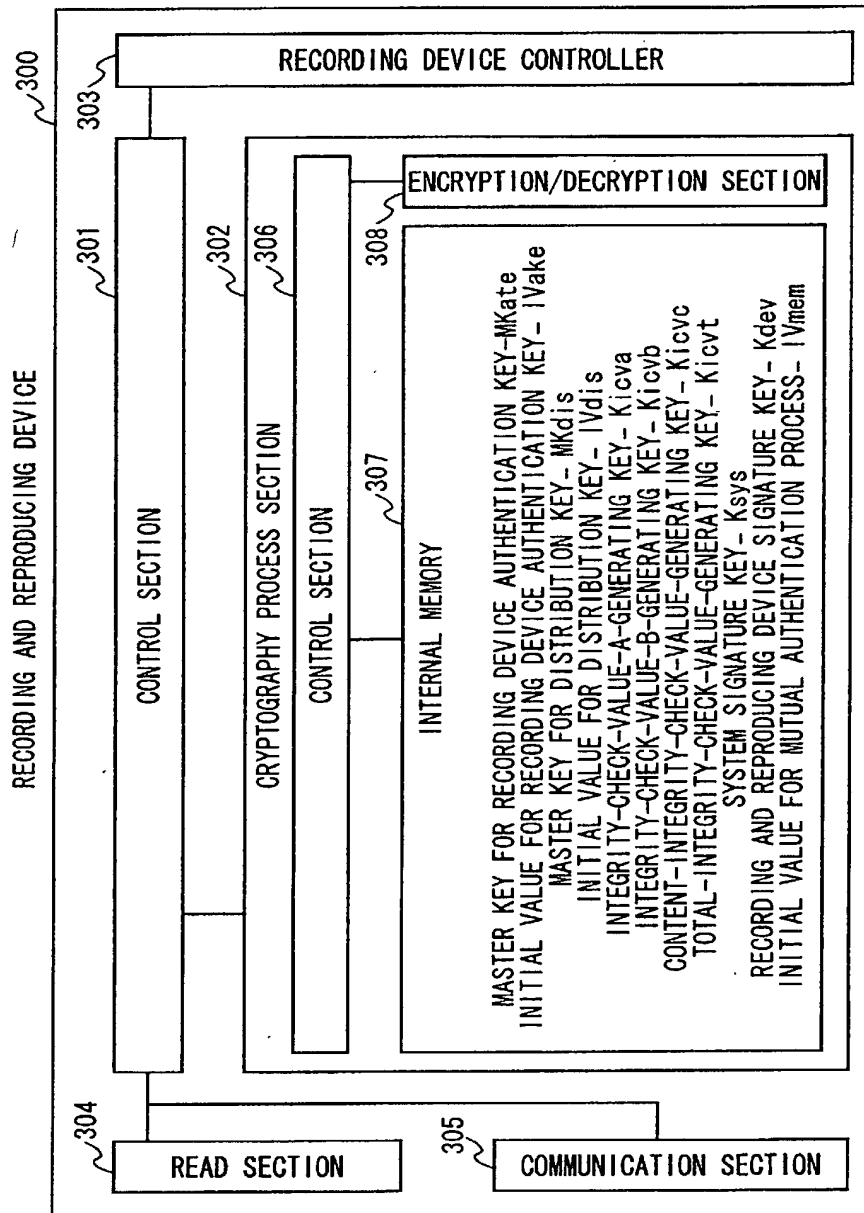
DECRYPTIONDECRYPTION USING ELLIPTIC CURVE CRYPTOGRAPHY (MENEZES-VANSTONE)

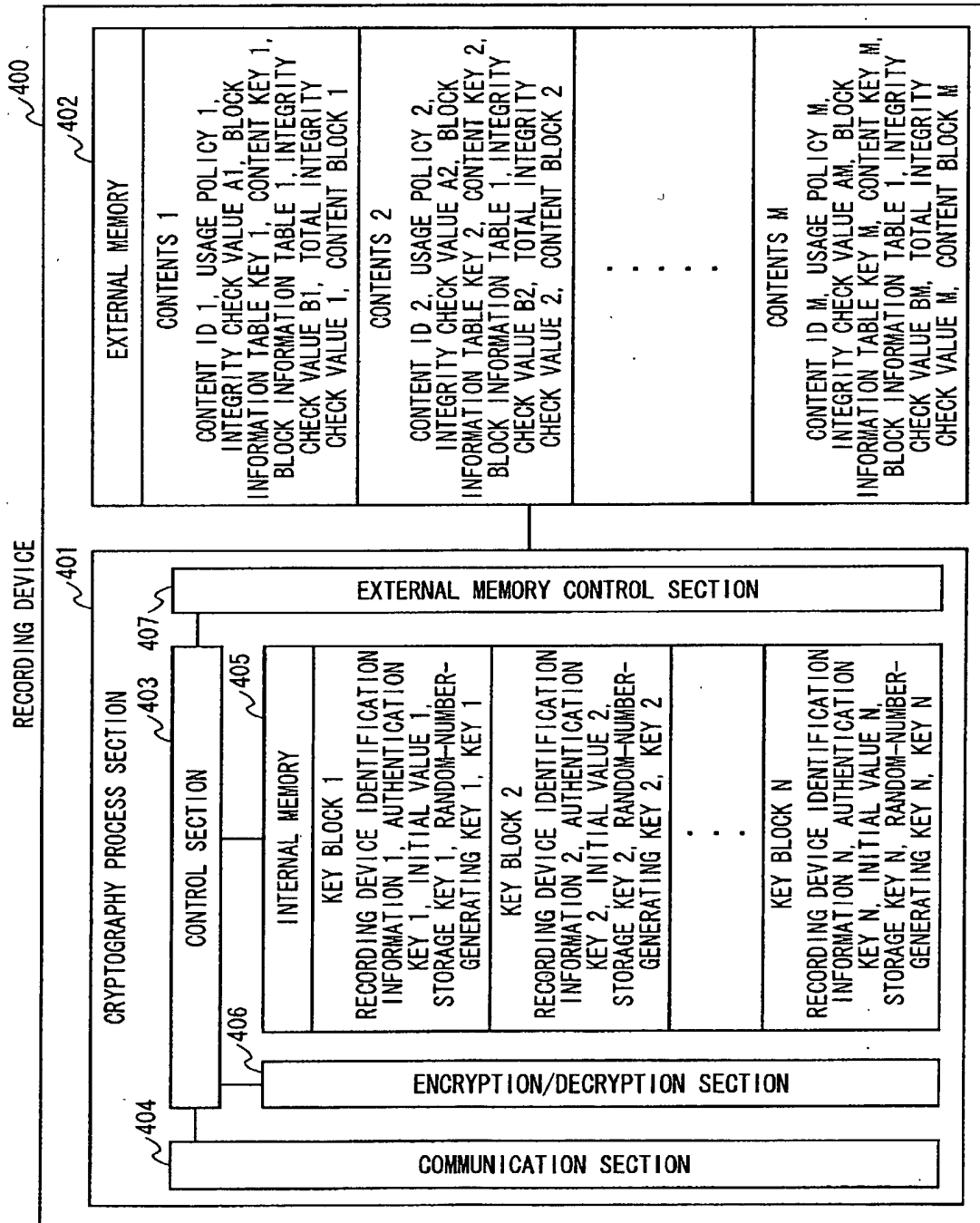
FIG. 17



HOW DATA ARE HELD ON RECORDING AND REPRODUCING DEVICE

FIG. 18

TOP SECRET



HOW DATA ARE HELD ON RECORDING DEVICE FIG. 19

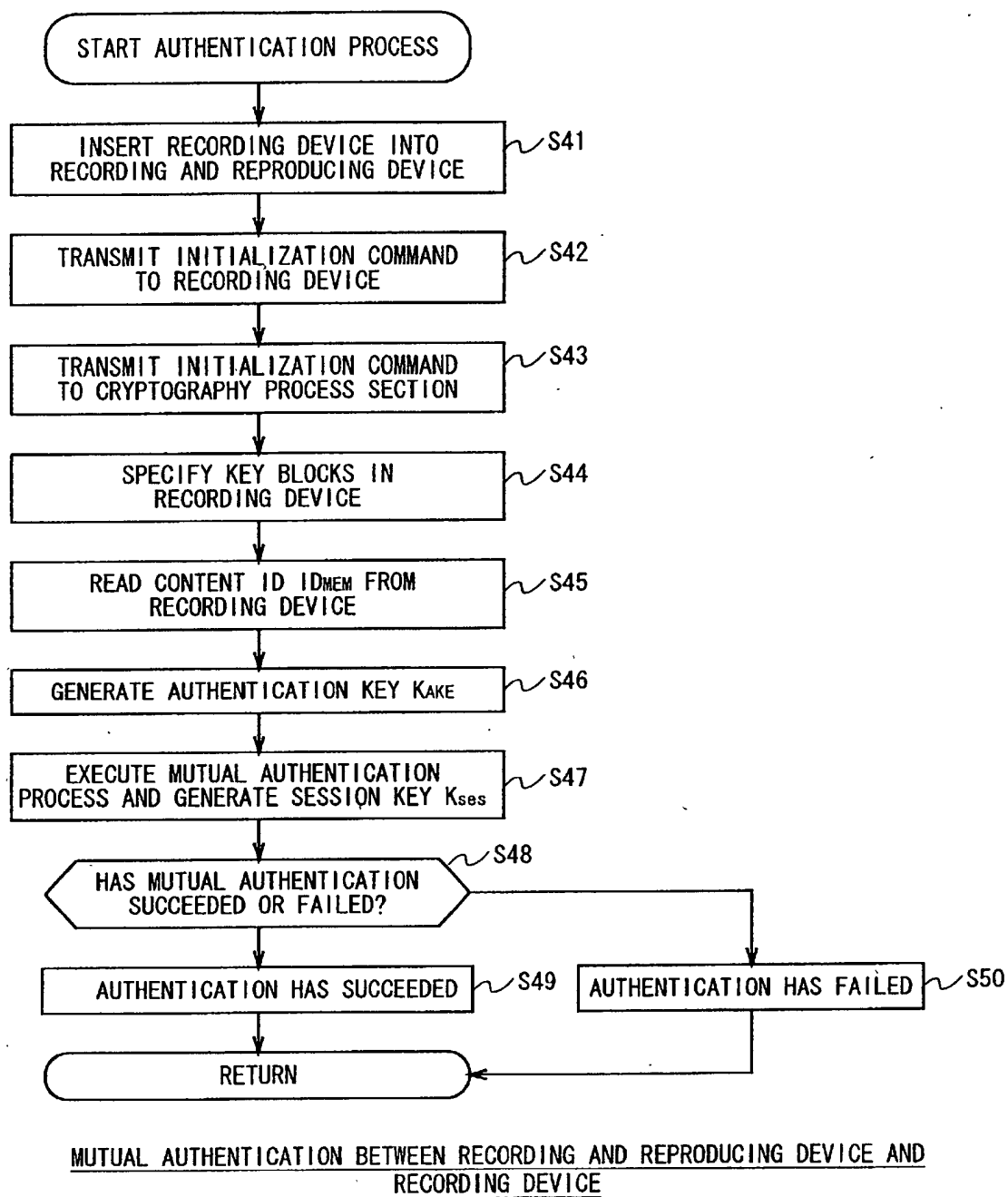


FIG. 20

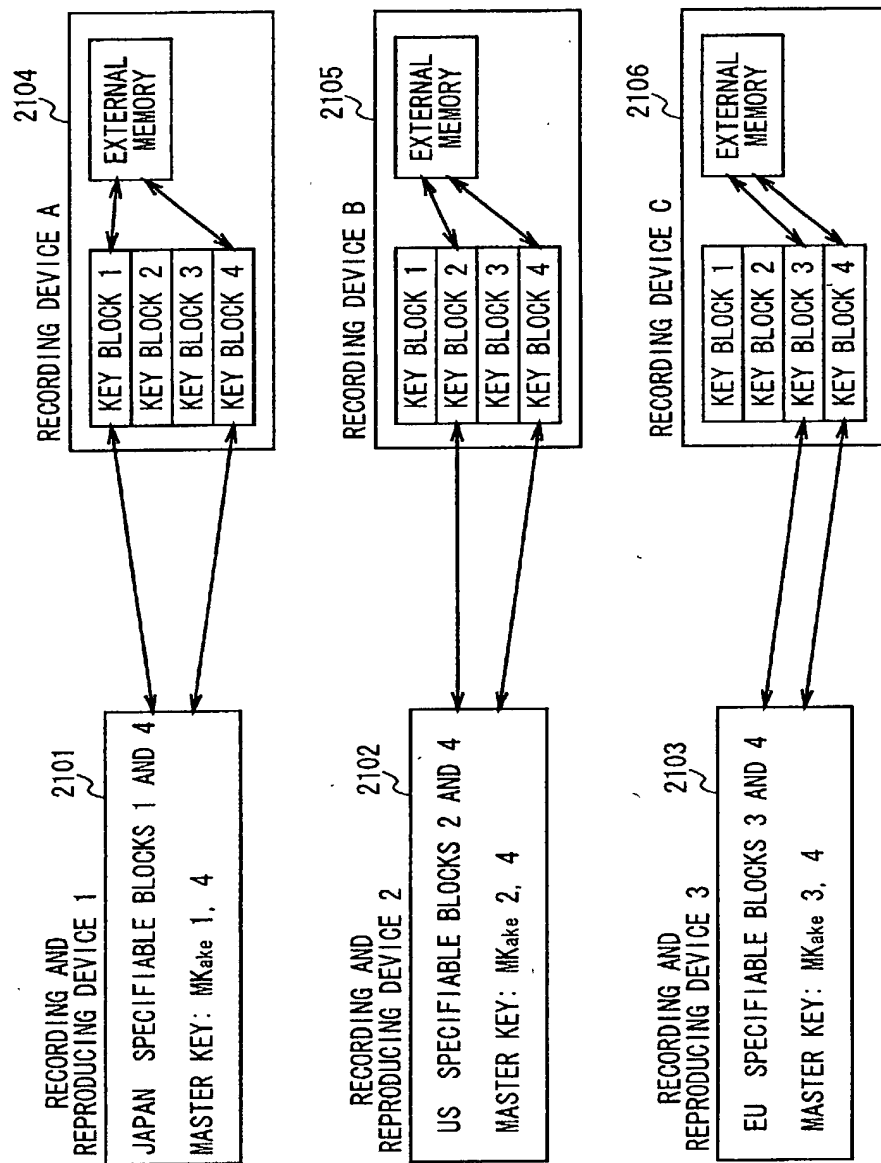
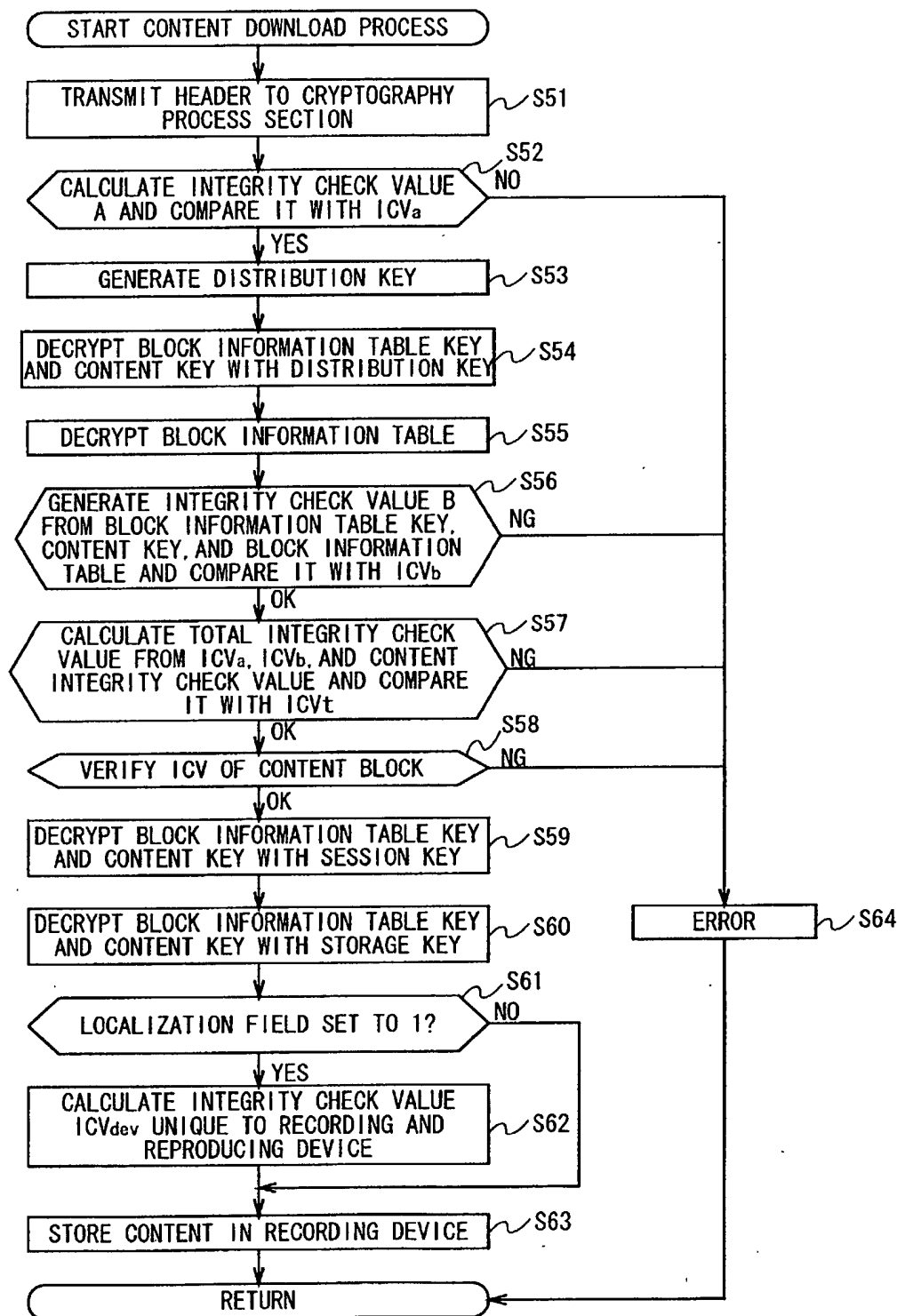
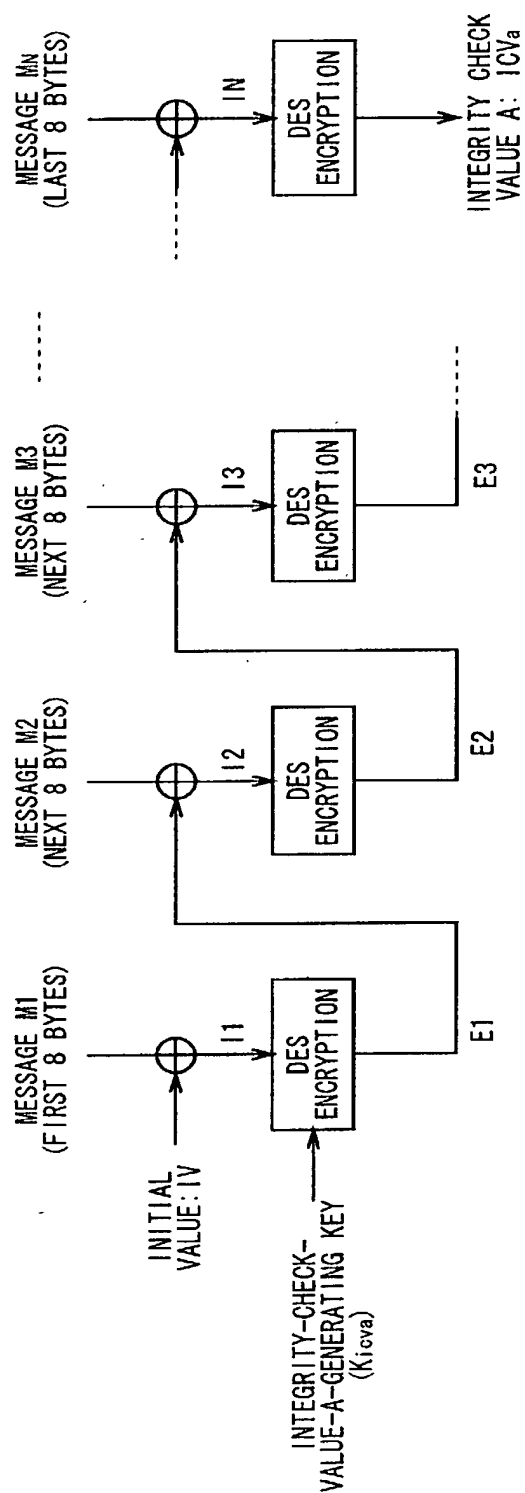


FIG. 21



CONTENT DOWNLOAD PROCESS

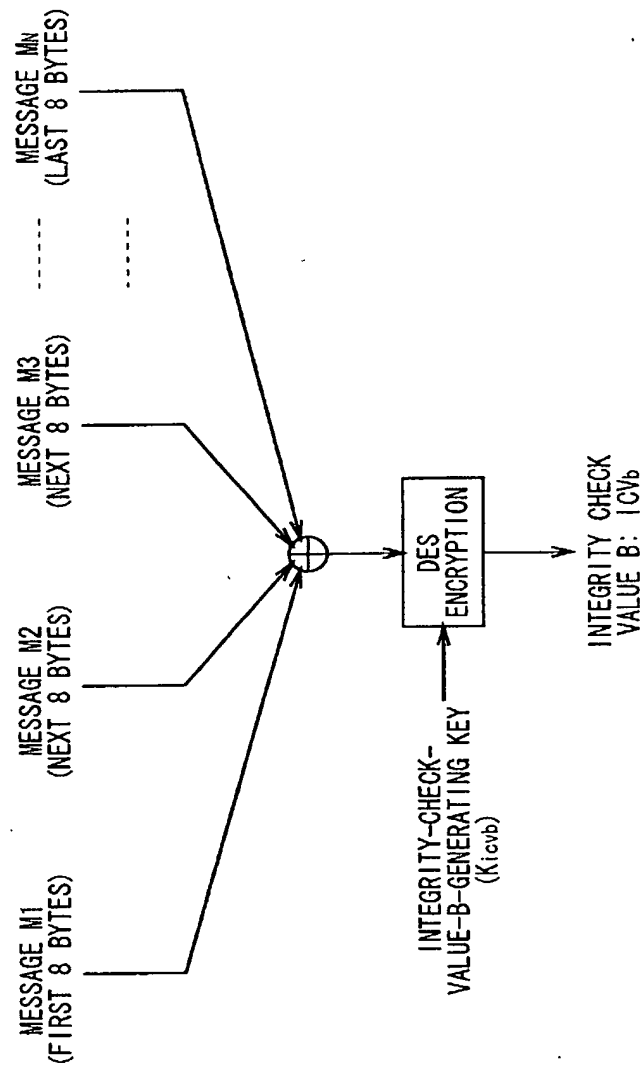
FIG. 22



MESSAGES M1 TO MN: CONTENT ID AND USAGE POLICY

⊕: EXCLUSIVE OR PROCESS (EVERY 8 BYTES)

FIG. 23



MESSAGES M1 TO Mn: BLOCK INFORMATION TABLE KEY  $K_{bit}$ , CONTENT KEY  $K_{con}$ , AND BLOCK INFORMATION TABLE  
 $\oplus$ : EXCLUSIVE OR PROCESS (EVERY 8 BYTES)

FIG. 24



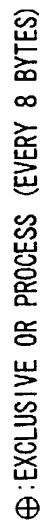
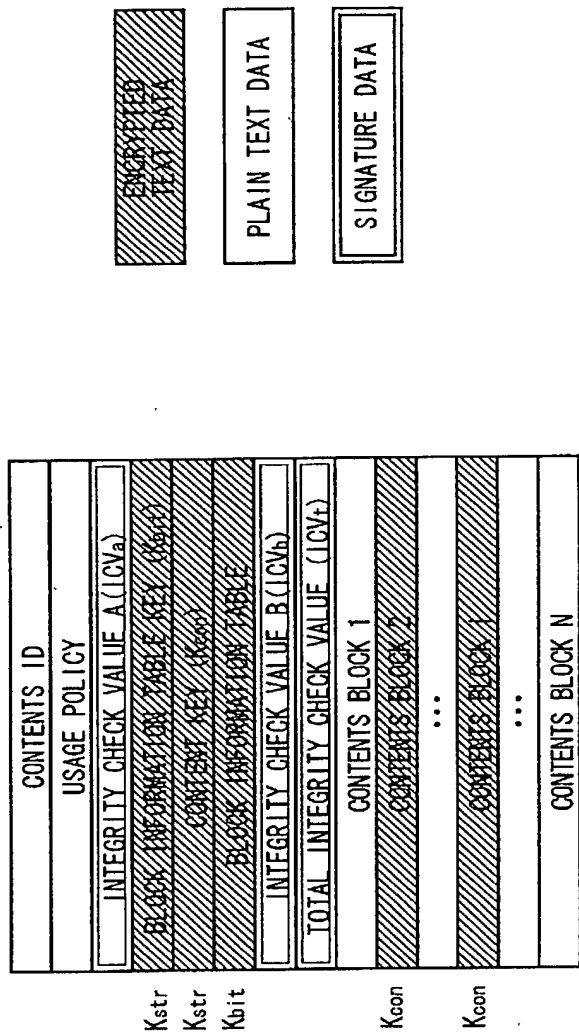


FIG. 25

TOP SECRET 0212250



CONTENT STORED IN RECORDING DEVICE  
(LOCALIZATION FIELD = 0)

FIG. 26

FIG. 27

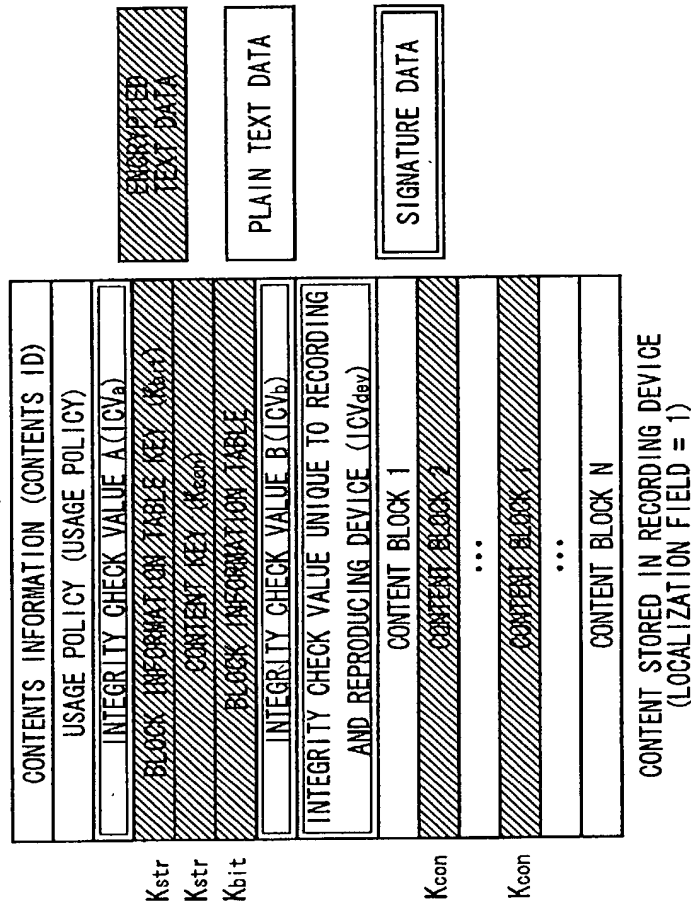


FIG. 27

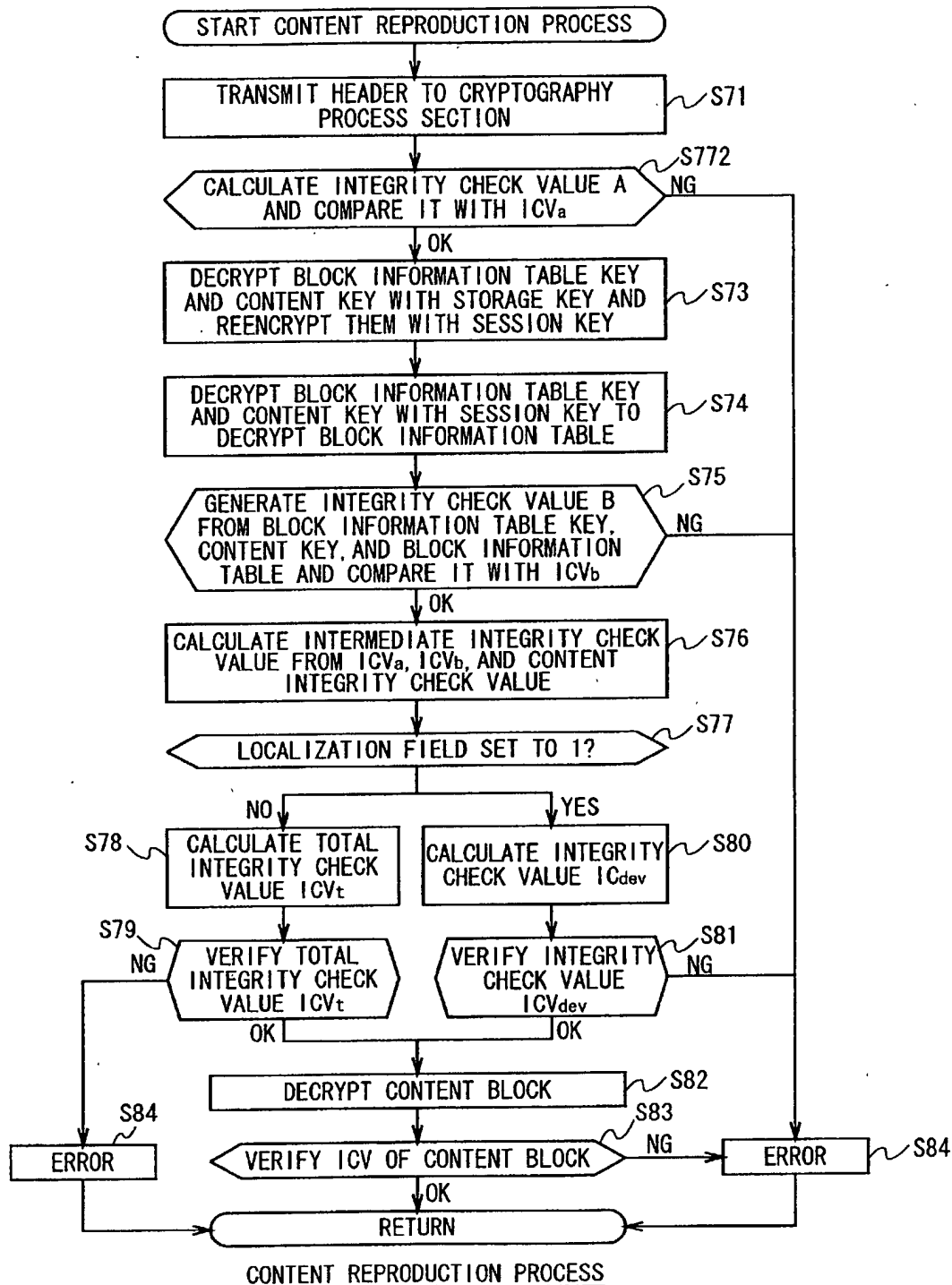


FIG. 28

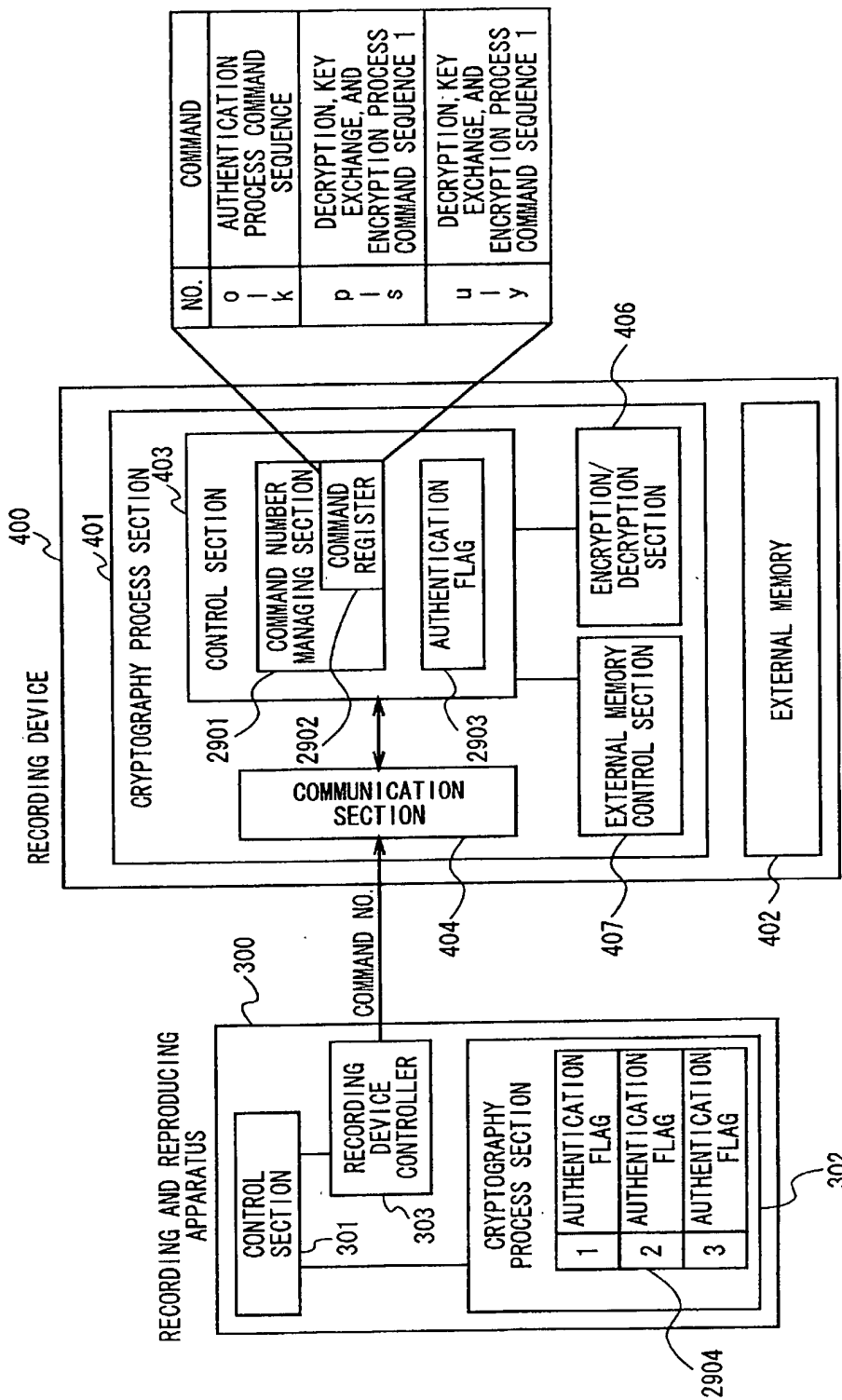


FIG. 29

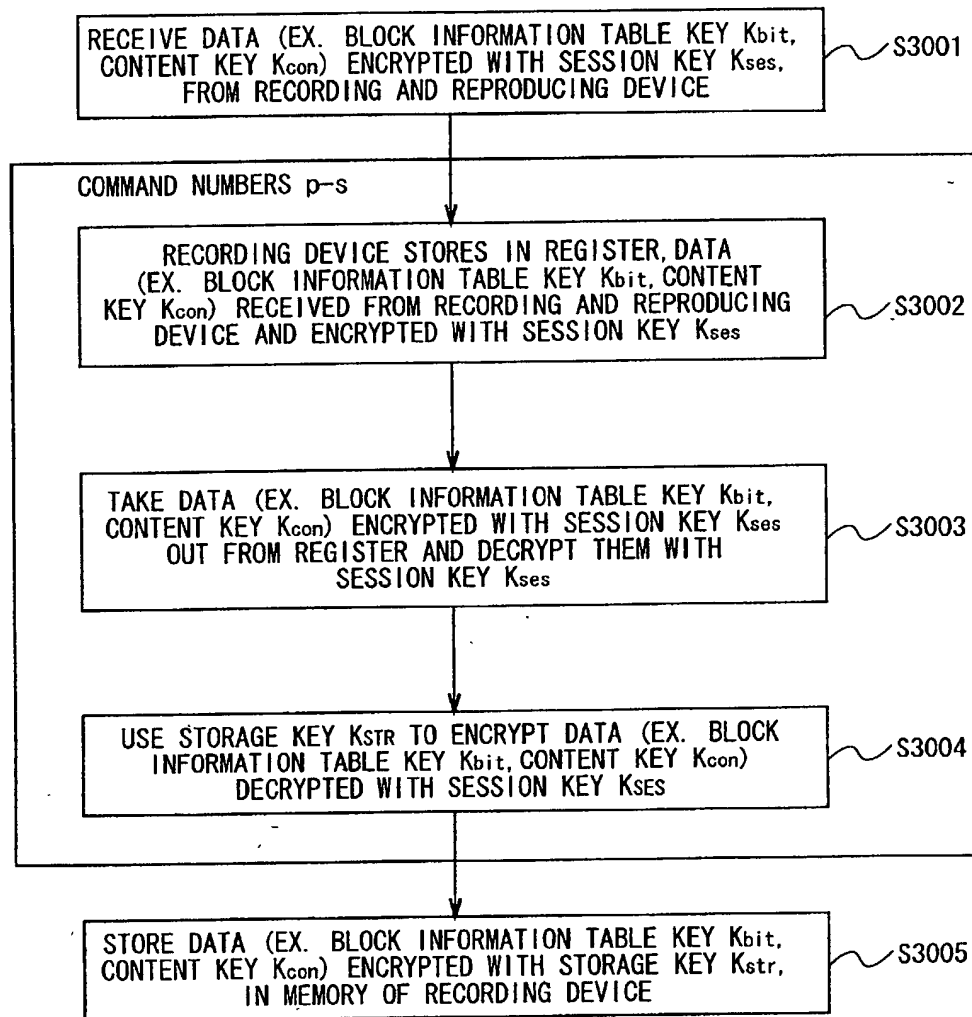


FIG. 30

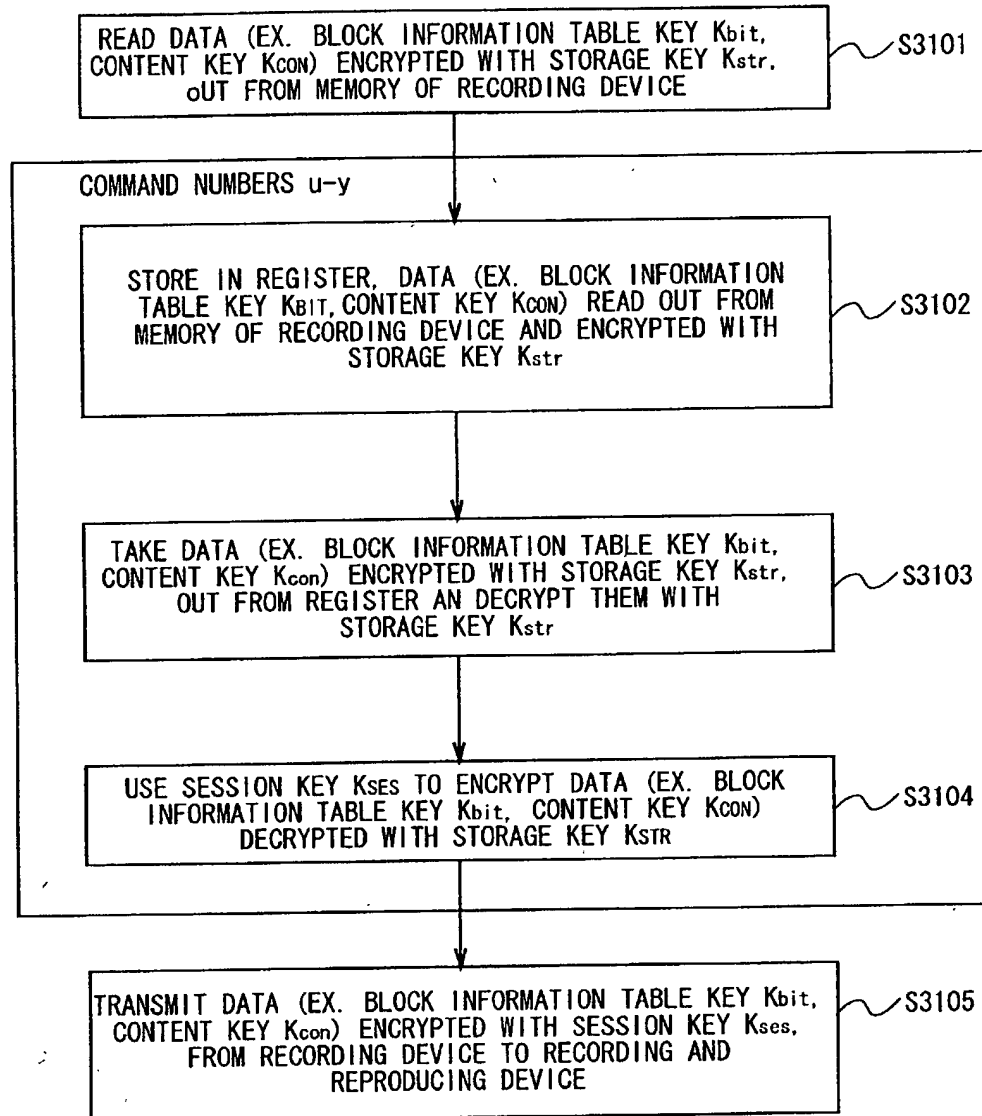


FIG. 31

FORMAT TYPE 0

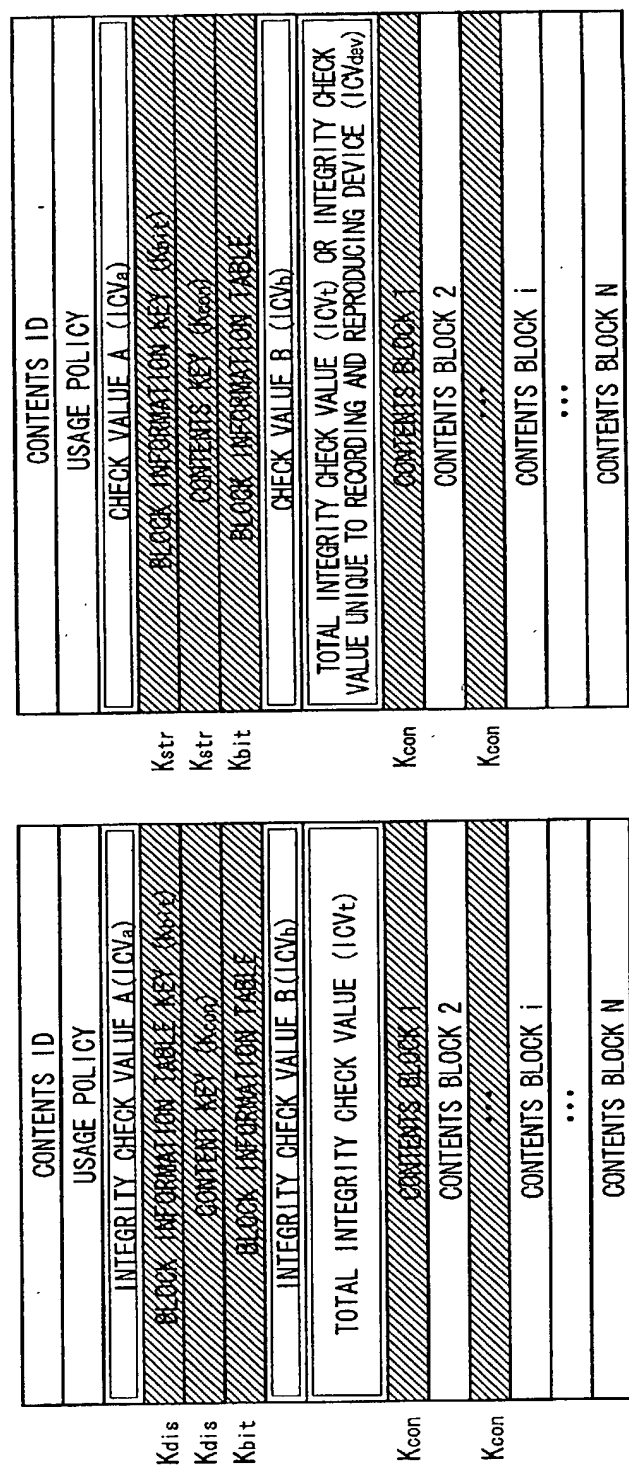


FIG. 32

09/937120



FOUO 00000000

FORMAT TYPE 1

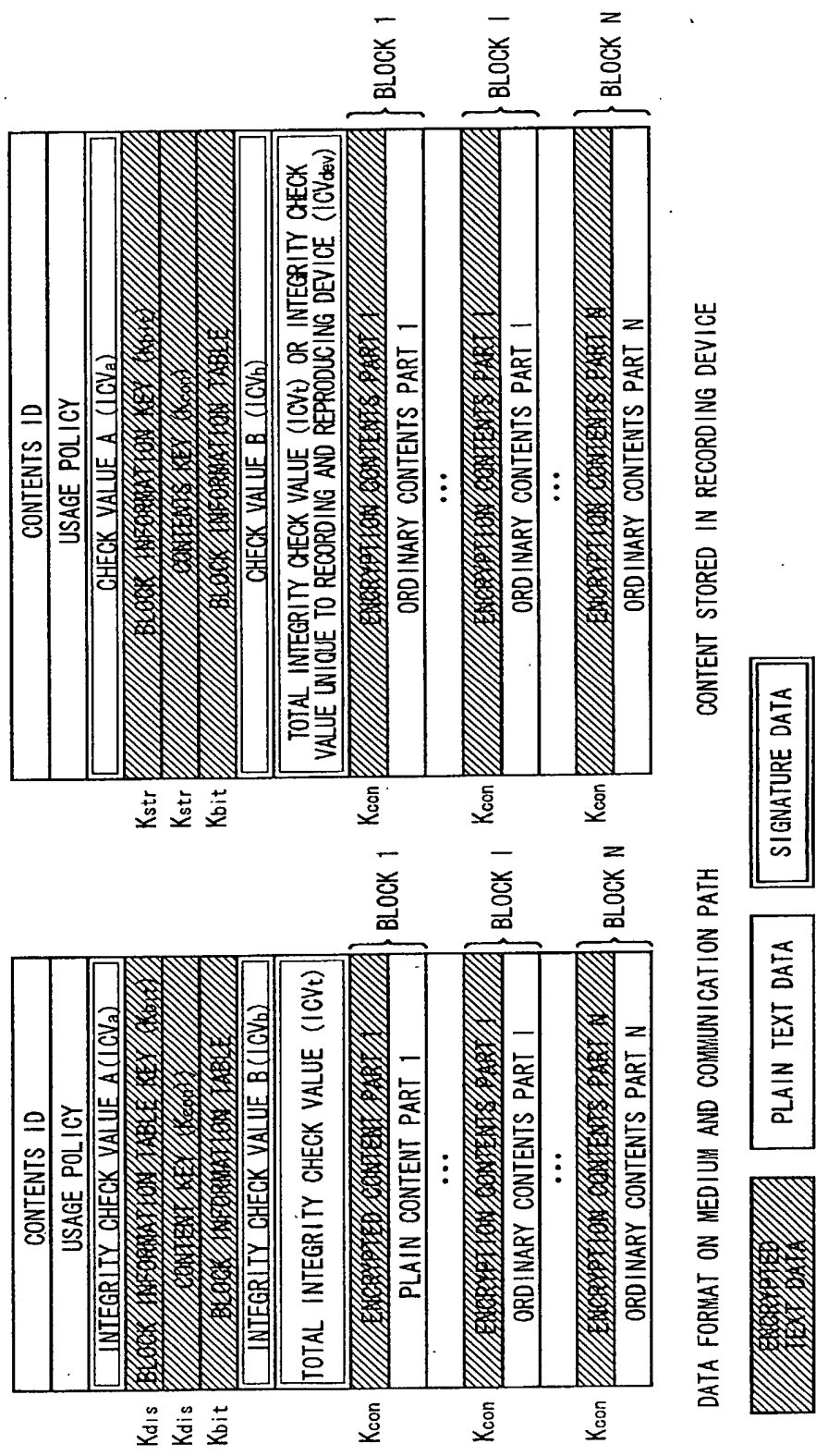


FIG. 33

FORMAT TYPE 2

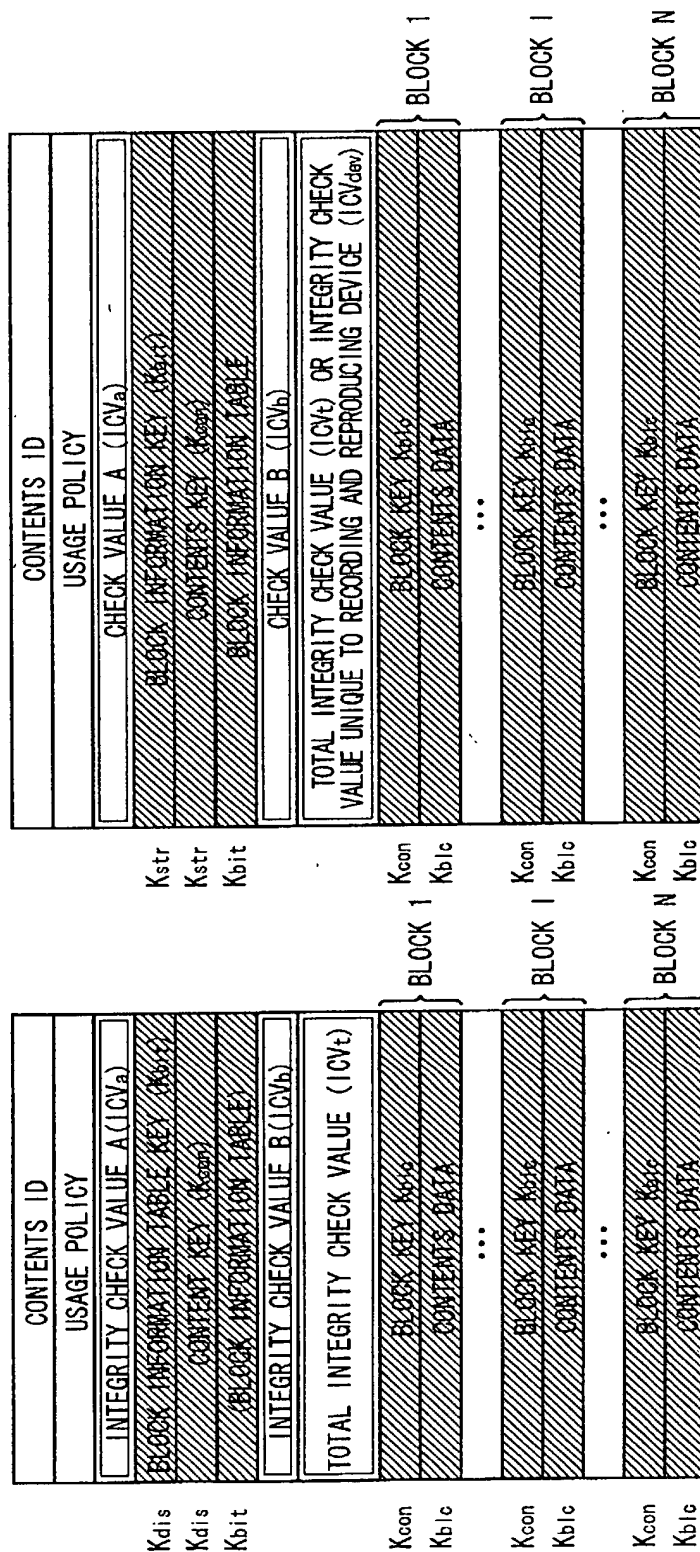


FIG. 34

FIG. 27-02F2E660

FORMAT TYPE 3

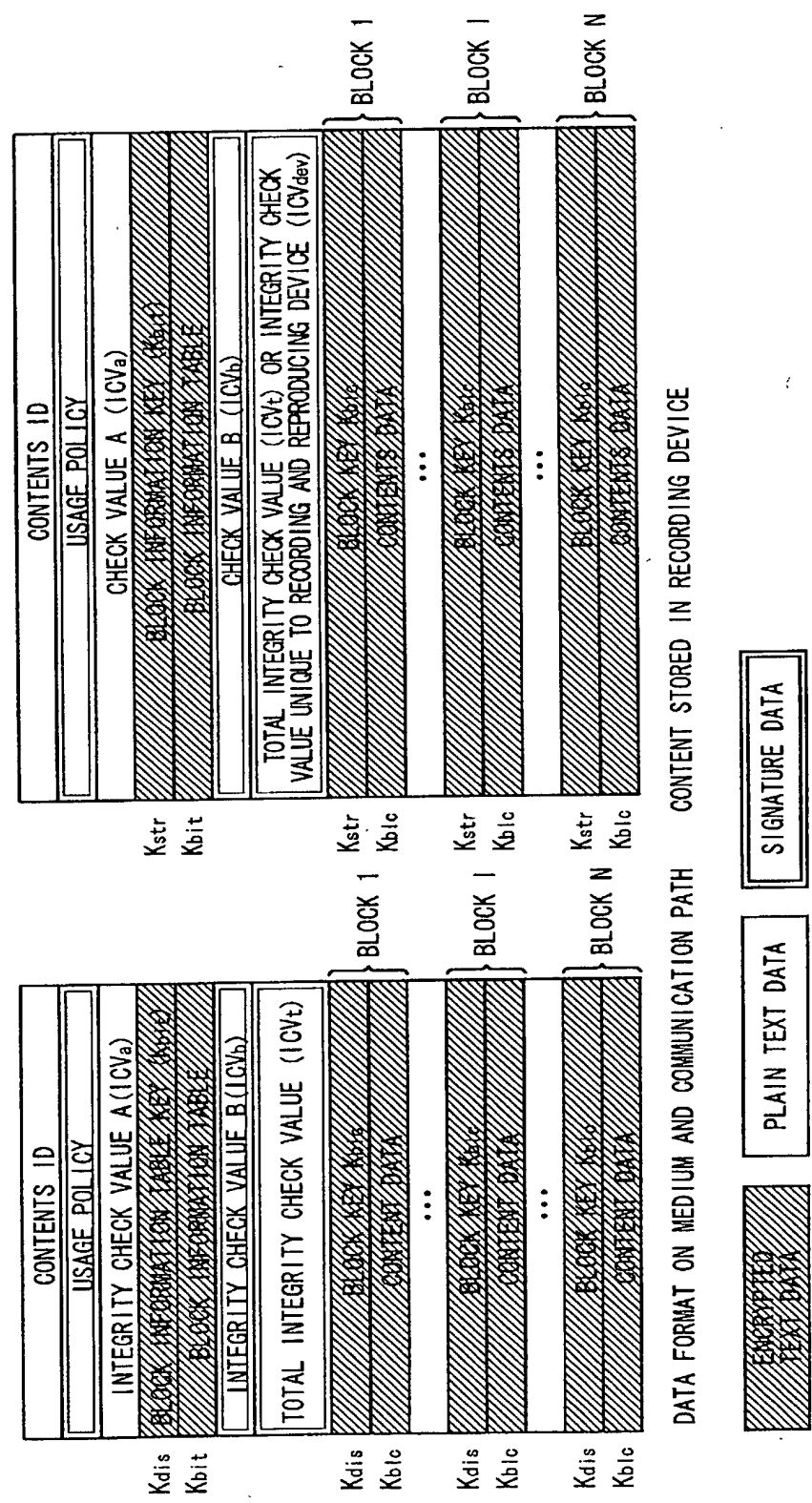
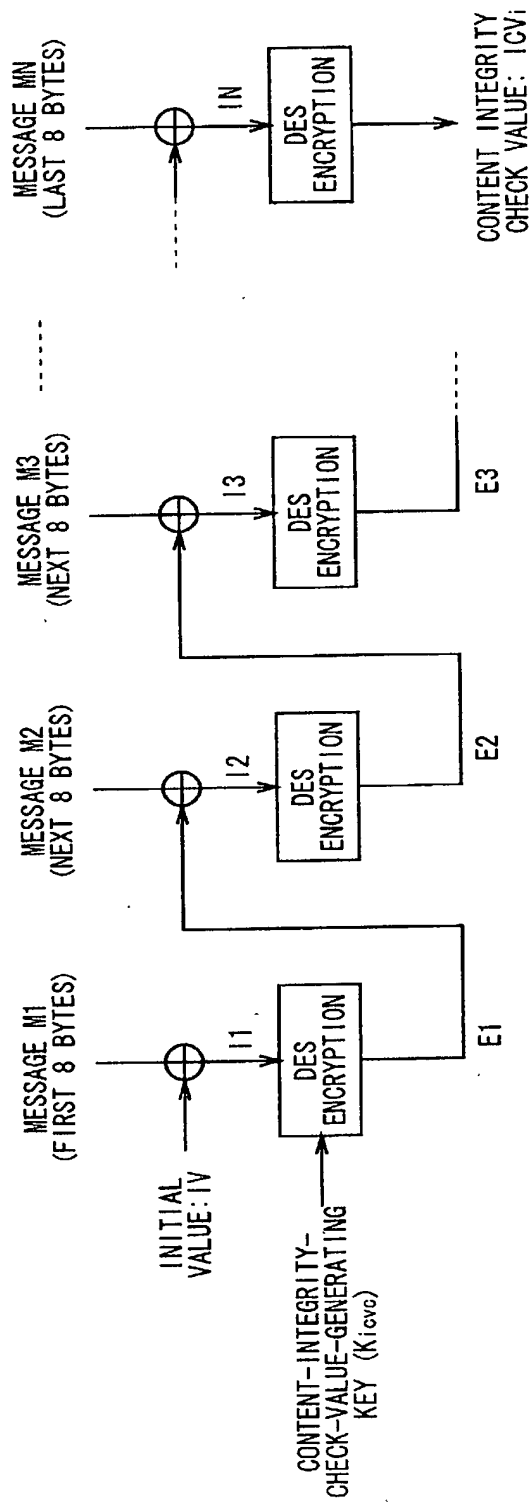


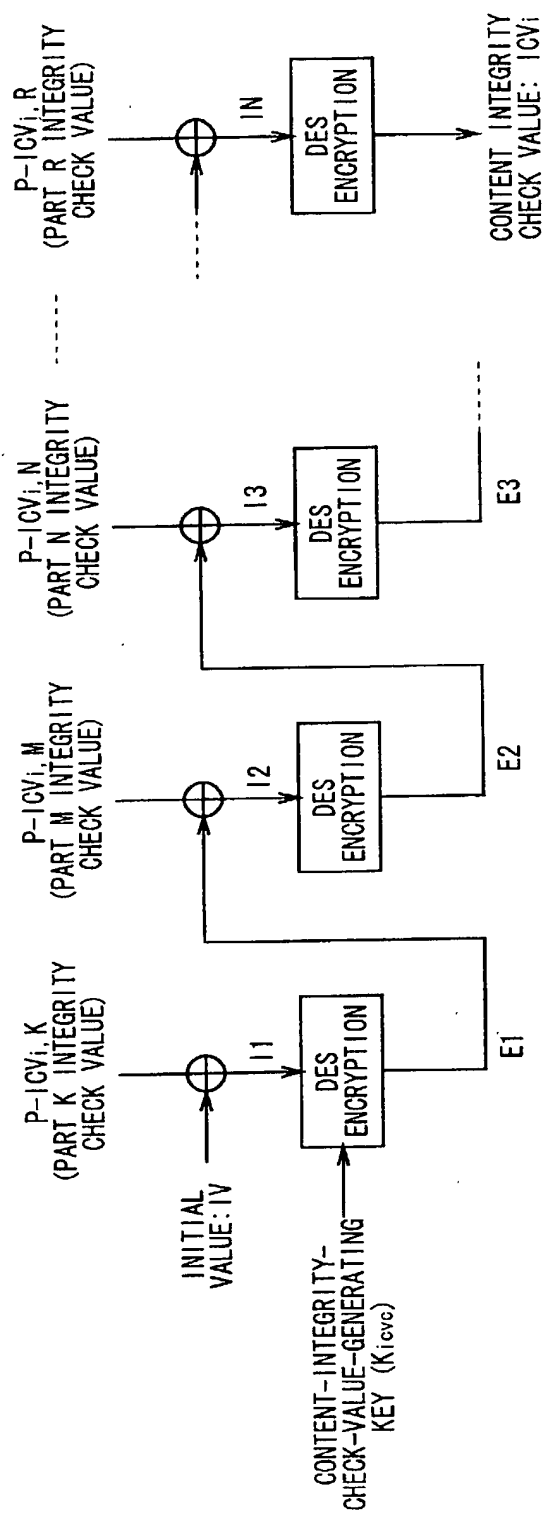
FIG. 35



MESSAGES M1 TO MN: CONTENT DATA IN CONTENT i

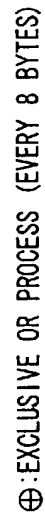
⊕: EXCLUSIVE OR PROCESS (EVERY 8 BYTES)

FIG. 36



$\oplus$  : EXCLUSIVE OR PROCESS (EVERY 8 BYTES)

FIG. 37



38/93

## FORMAT TYPE 0 AND 1 DOWNLOAD PROCESS

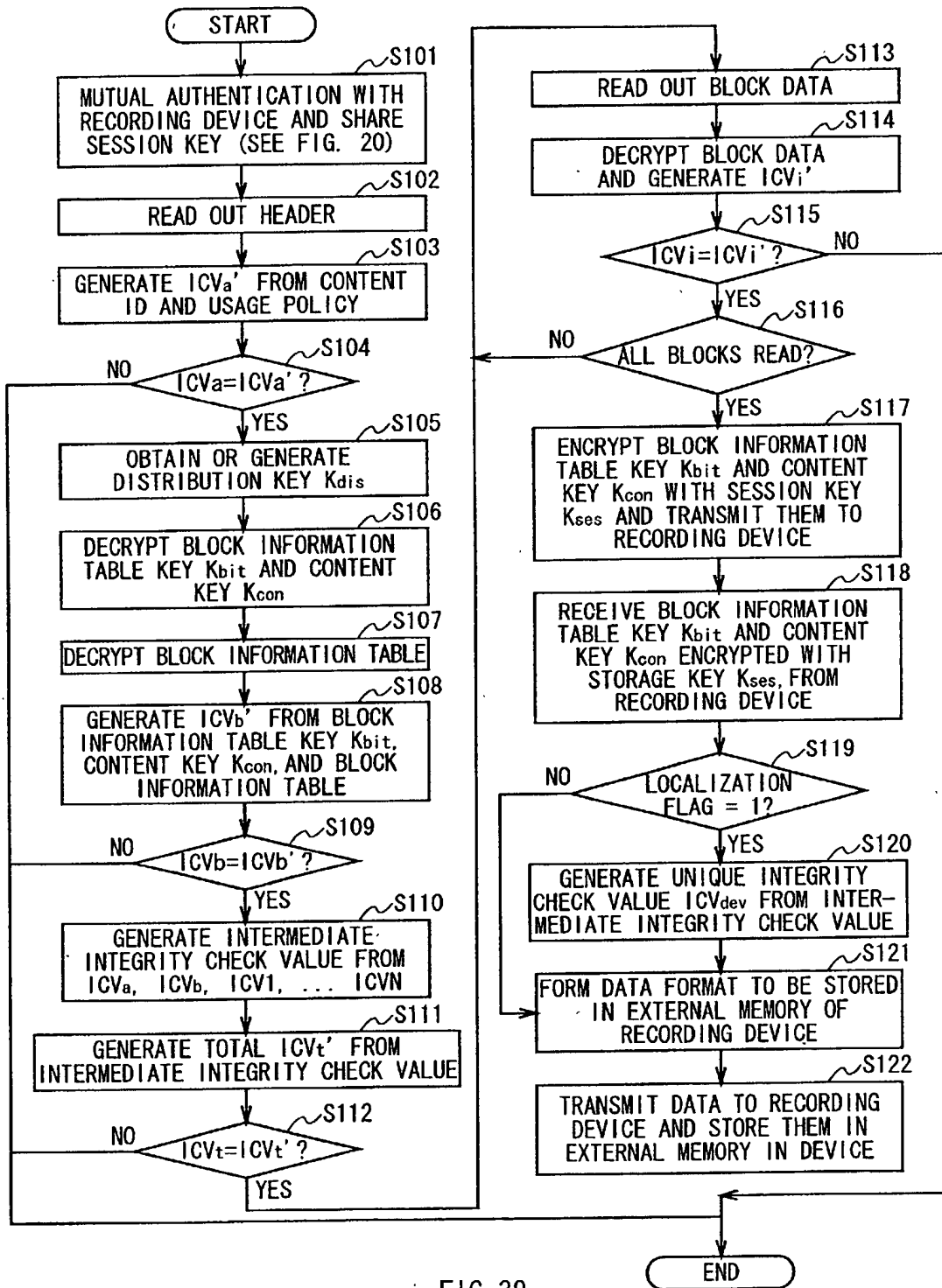


FIG. 39

## FORMAT TYPE 2 DOWNLOAD PROCESS

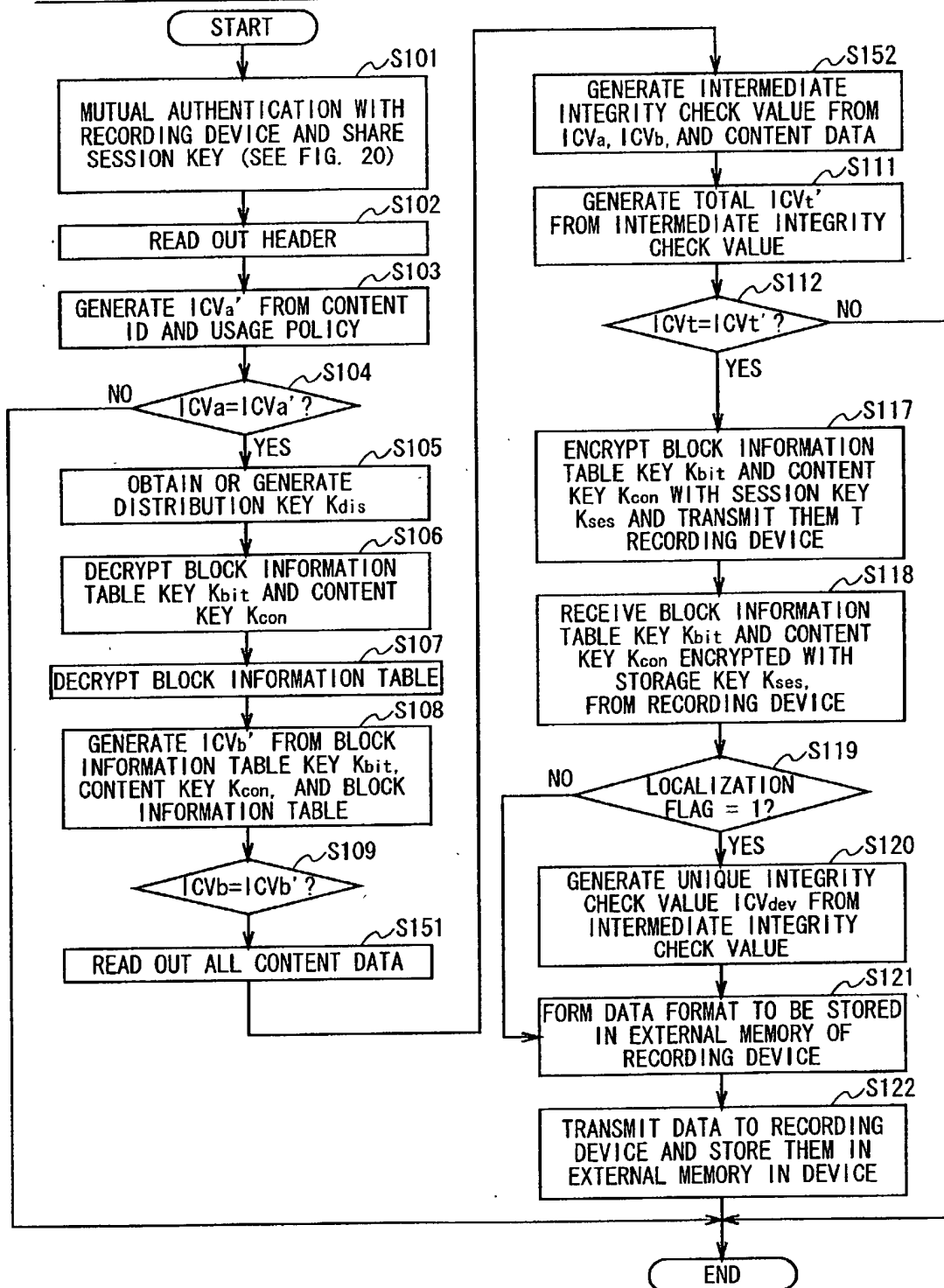


FIG. 40



## FORMAT TYPE 3 DOWNLOAD PROCESS

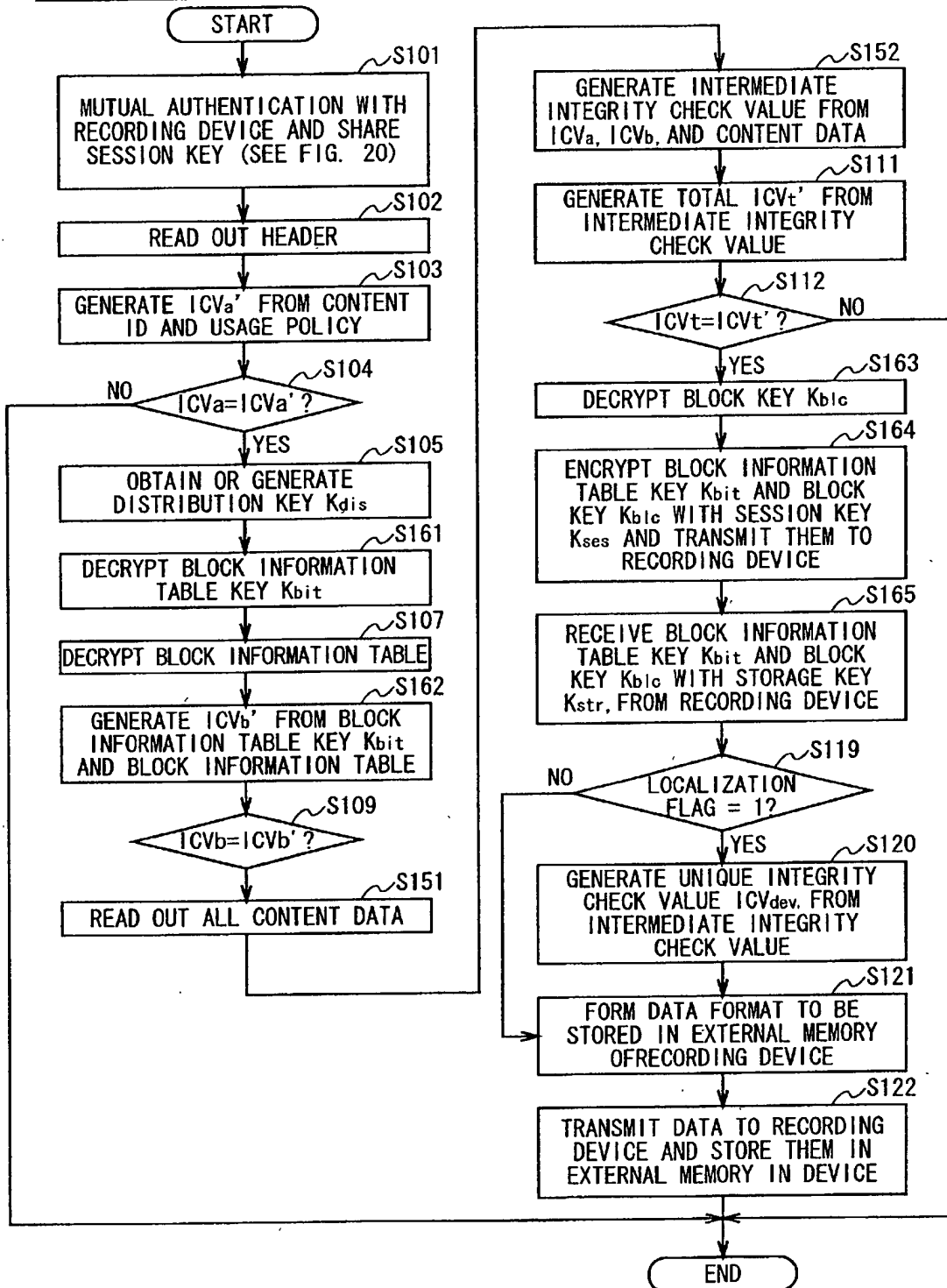
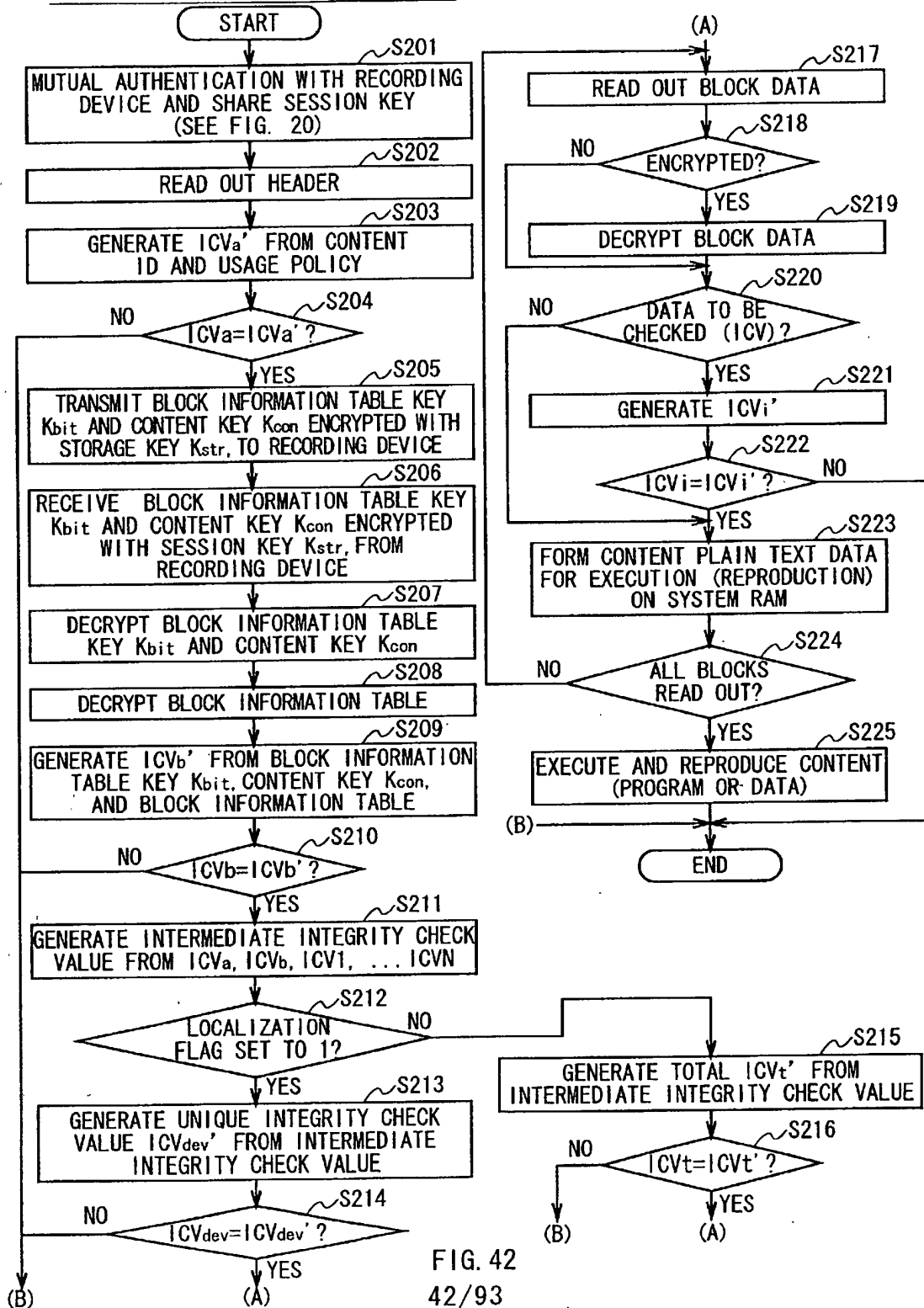
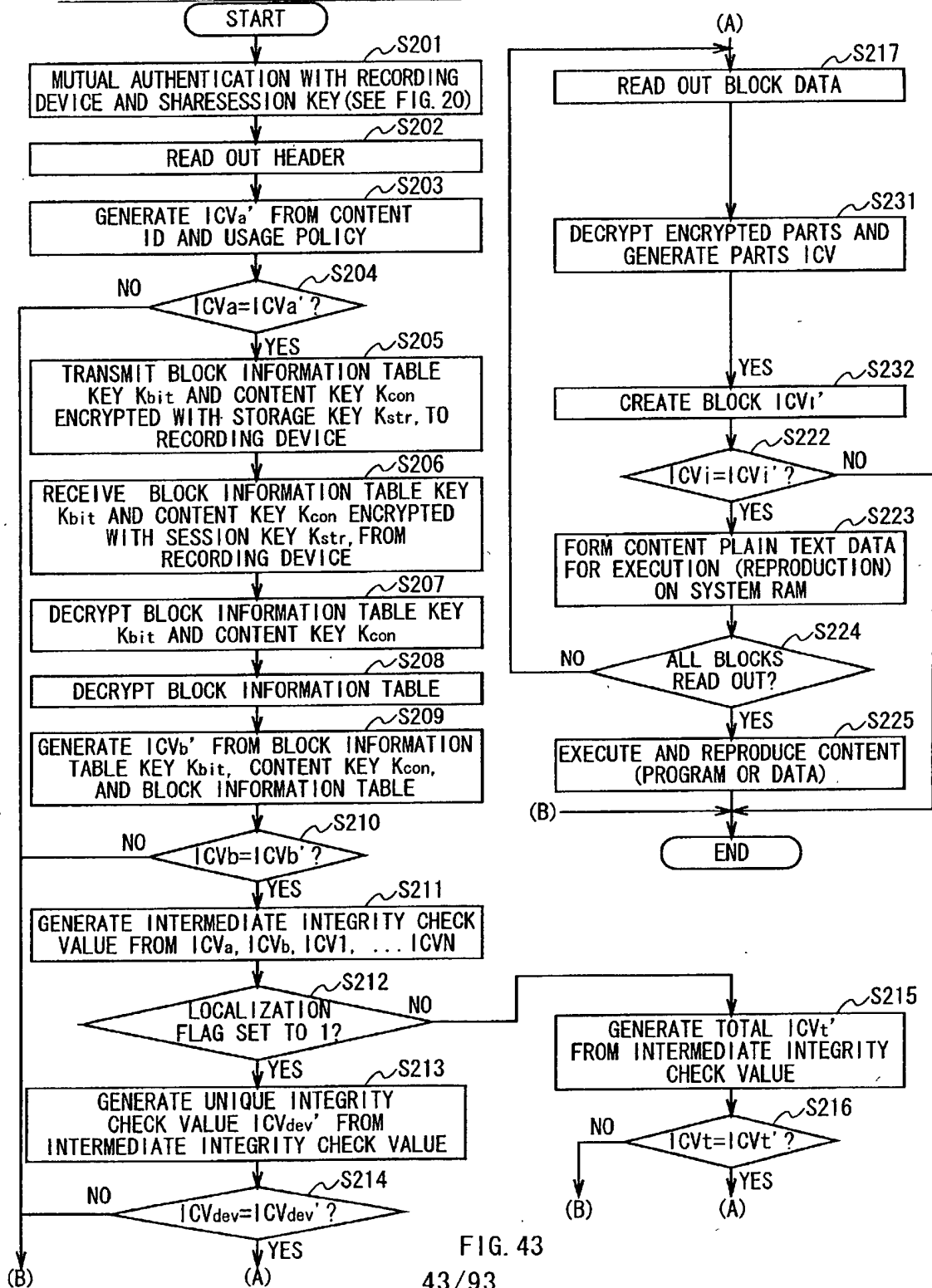


FIG. 41

## FORMAT TYPE 0 REPRODUCTION PROCESS

FIG. 42  
42/93

## FORMAT TYPE 1 REPRODUCTION PROCESS



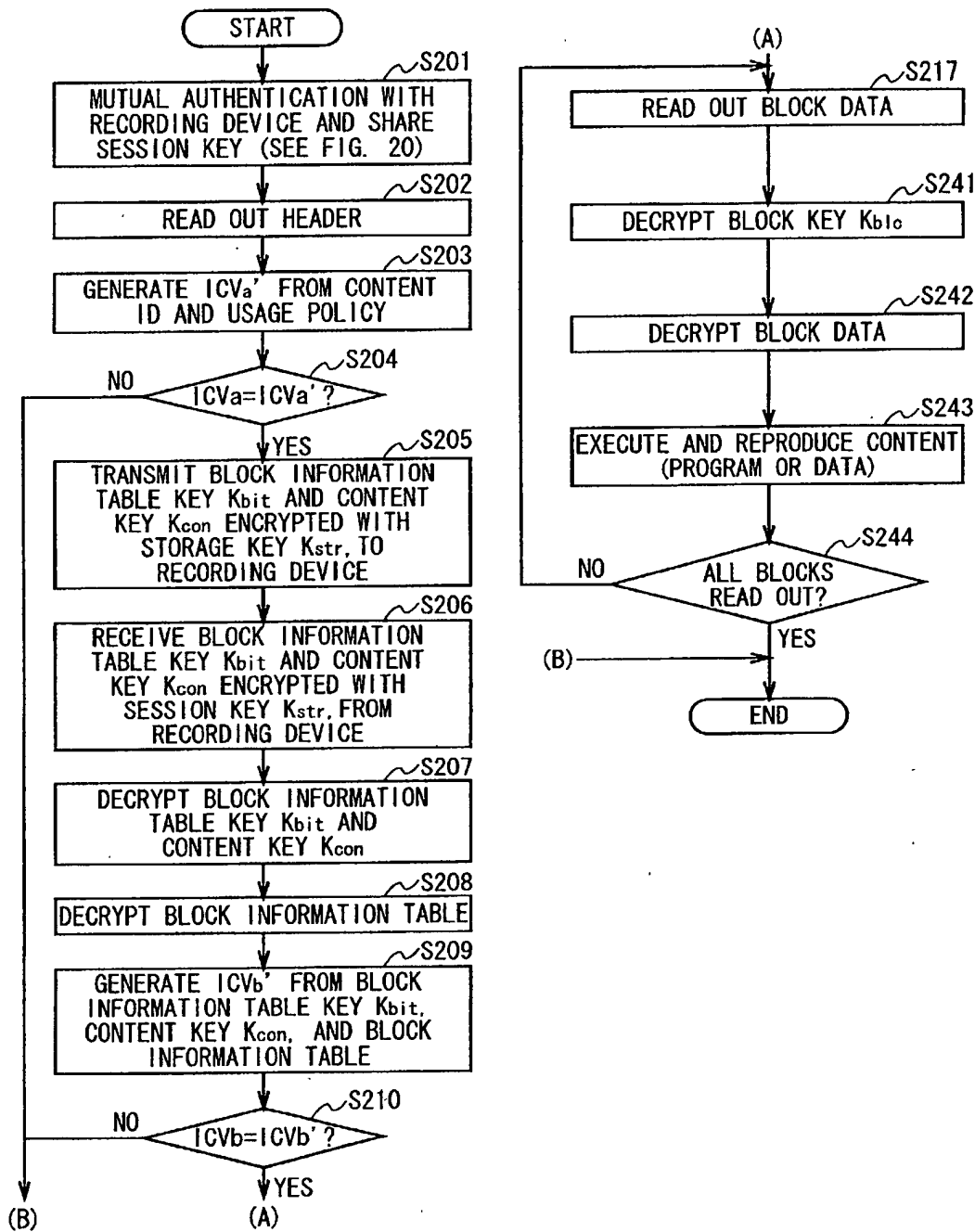


FIG. 44

## FORMAT TYPE 3 REPRODUCTION PROCESS

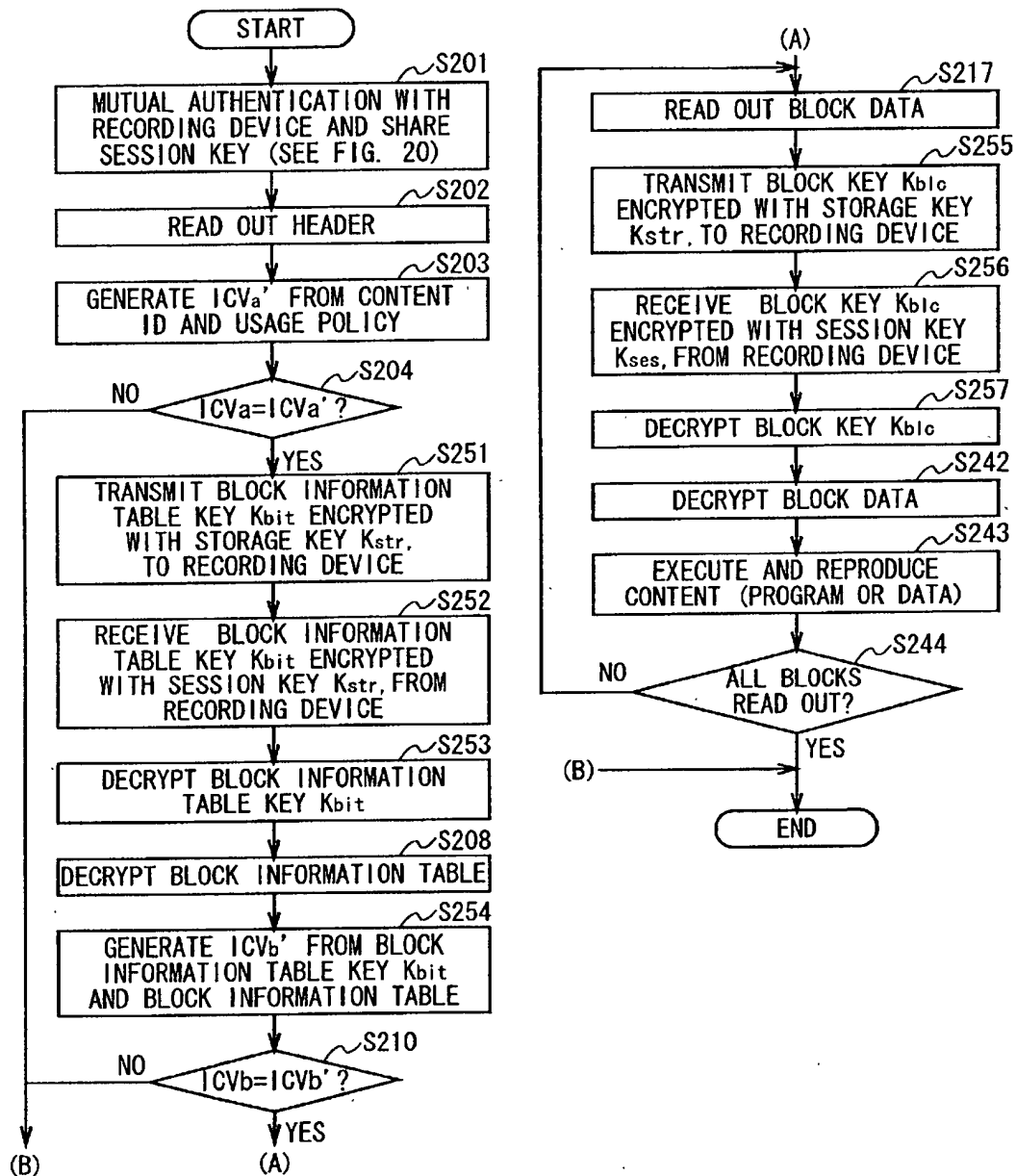


FIG. 45

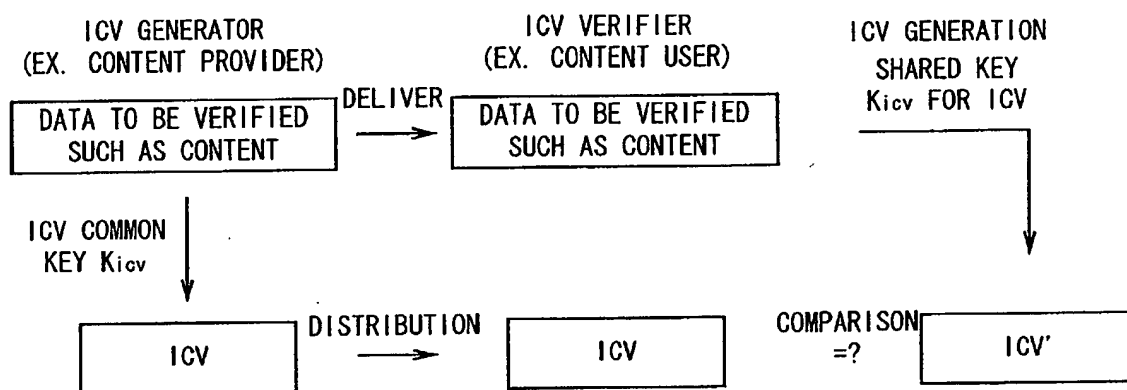


FIG. 46

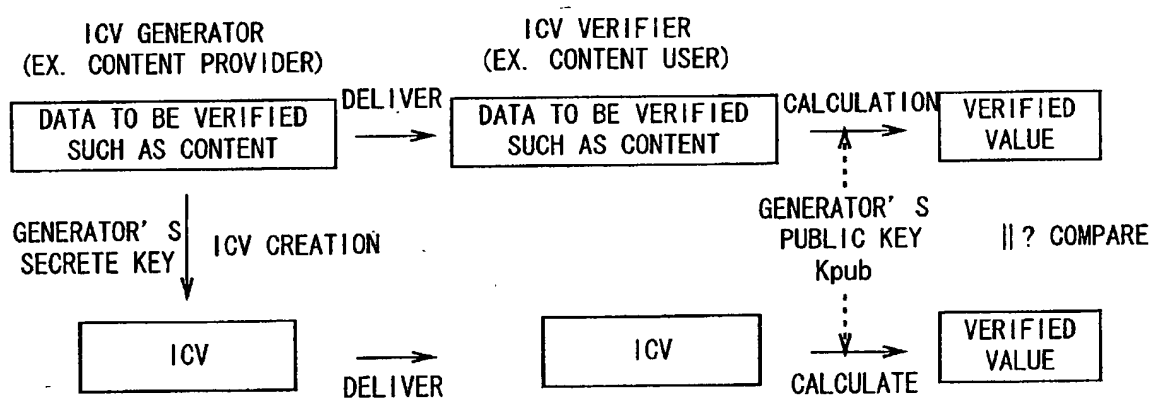


FIG. 47

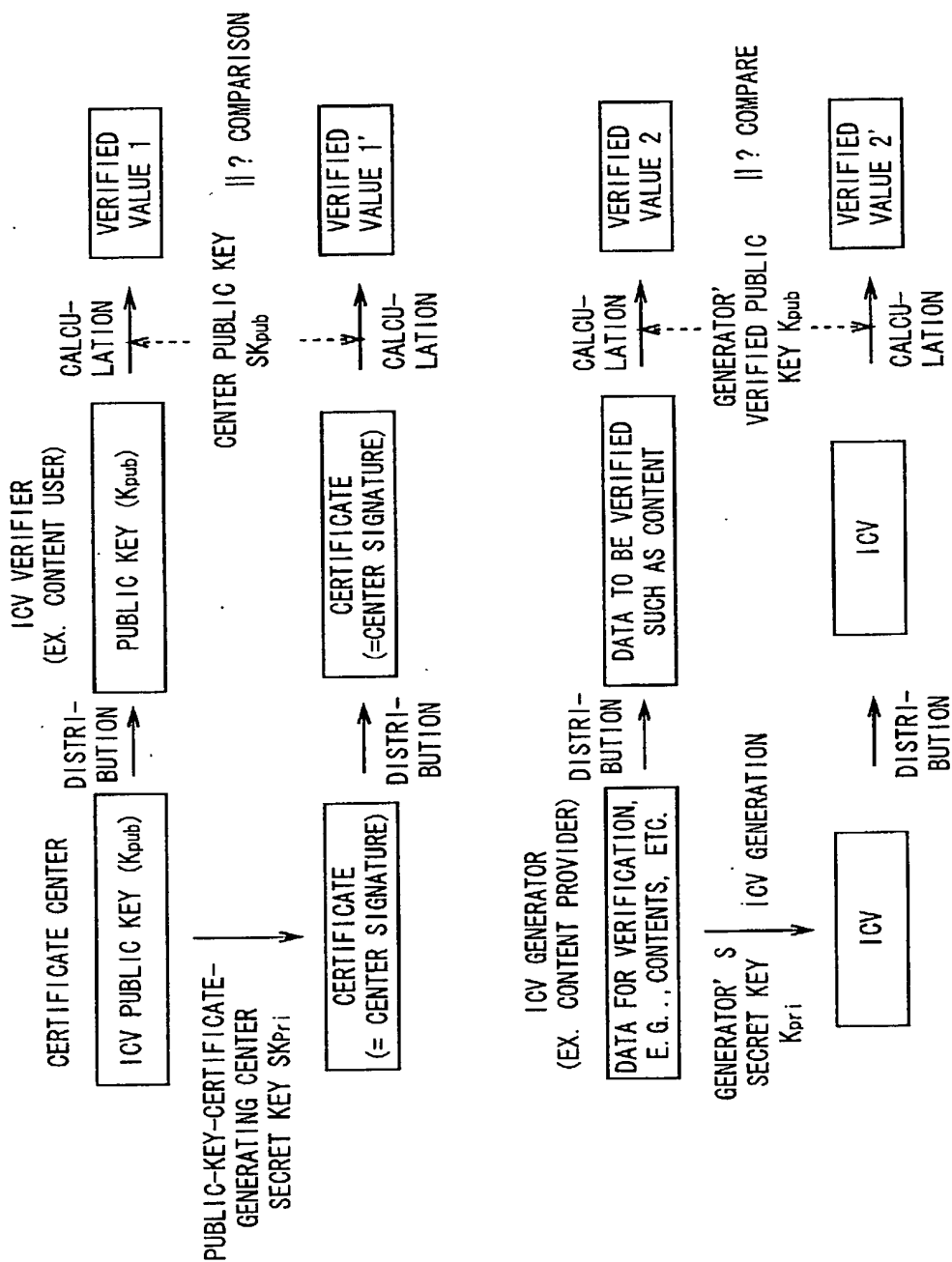


FIG. 48

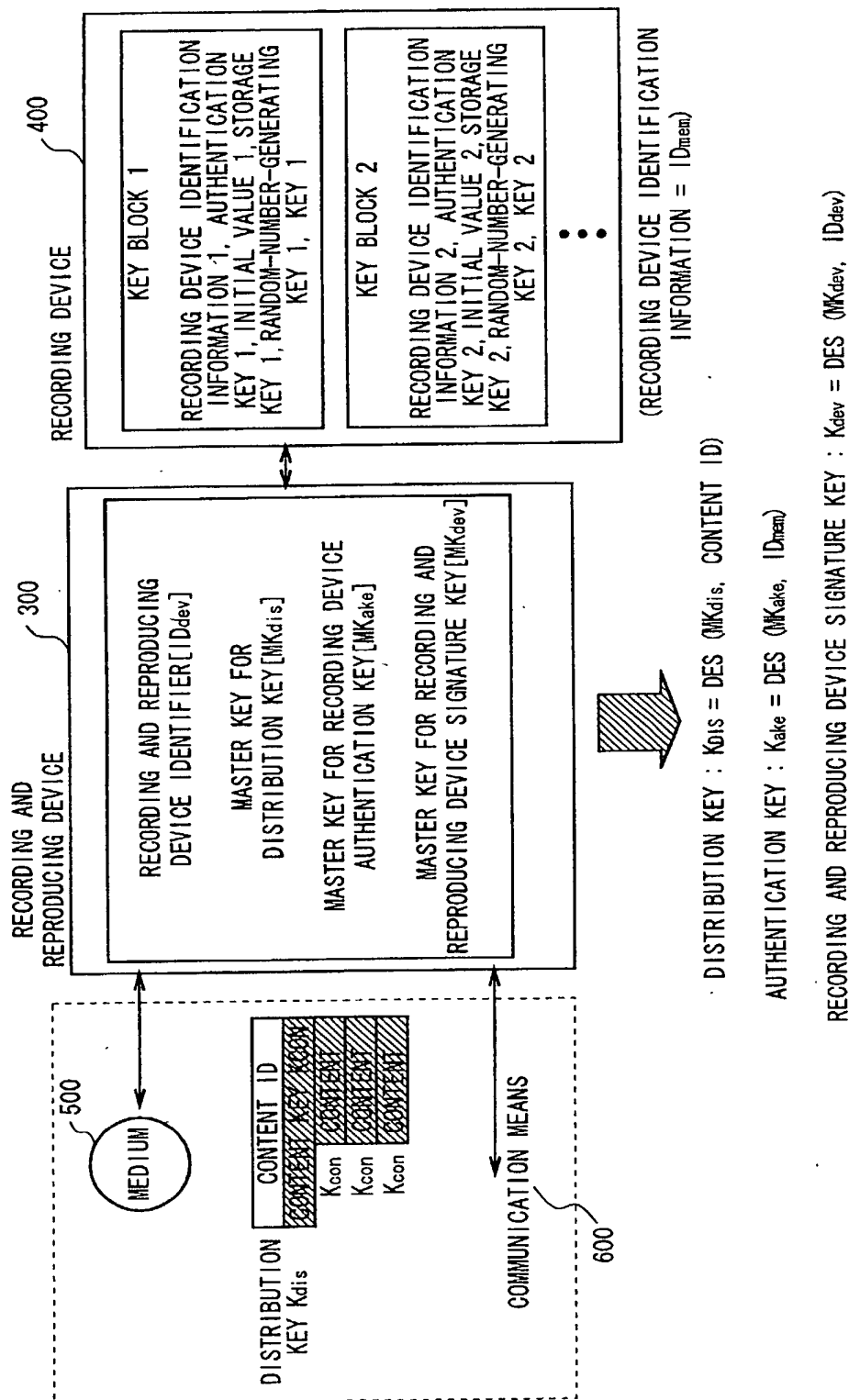


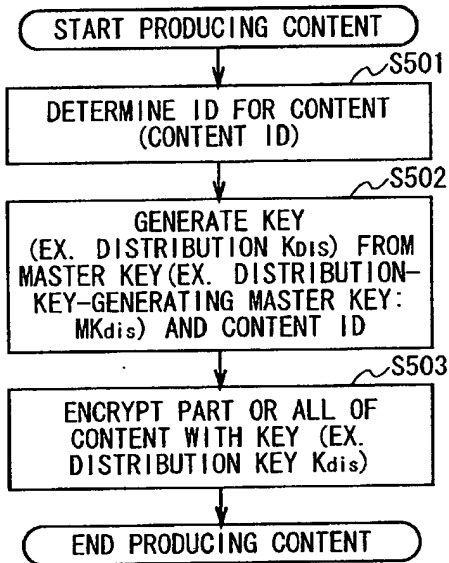
FIG. 49



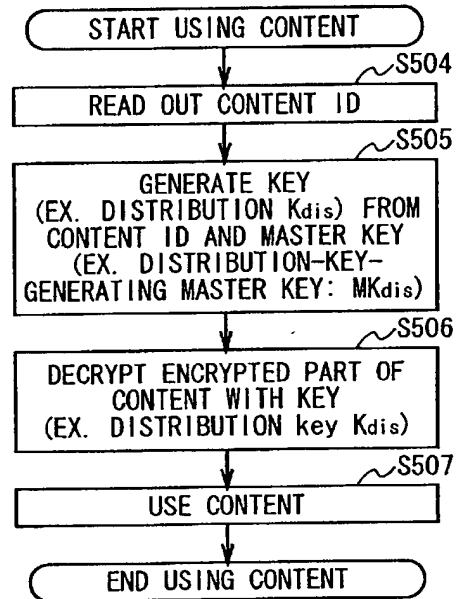
## METHOD FOR GENERATING INDIVIDUAL KEY FROM MASTER KEY - (1)

## [BASIC FLOW]

## CONTENT PRODUCER OR MANAGER



## USER DEVICE



## [KEY OWNER CONFIGURATION]

## CONTENT PRODUCER OR MANAGER



SHARE

## USER DEVICE

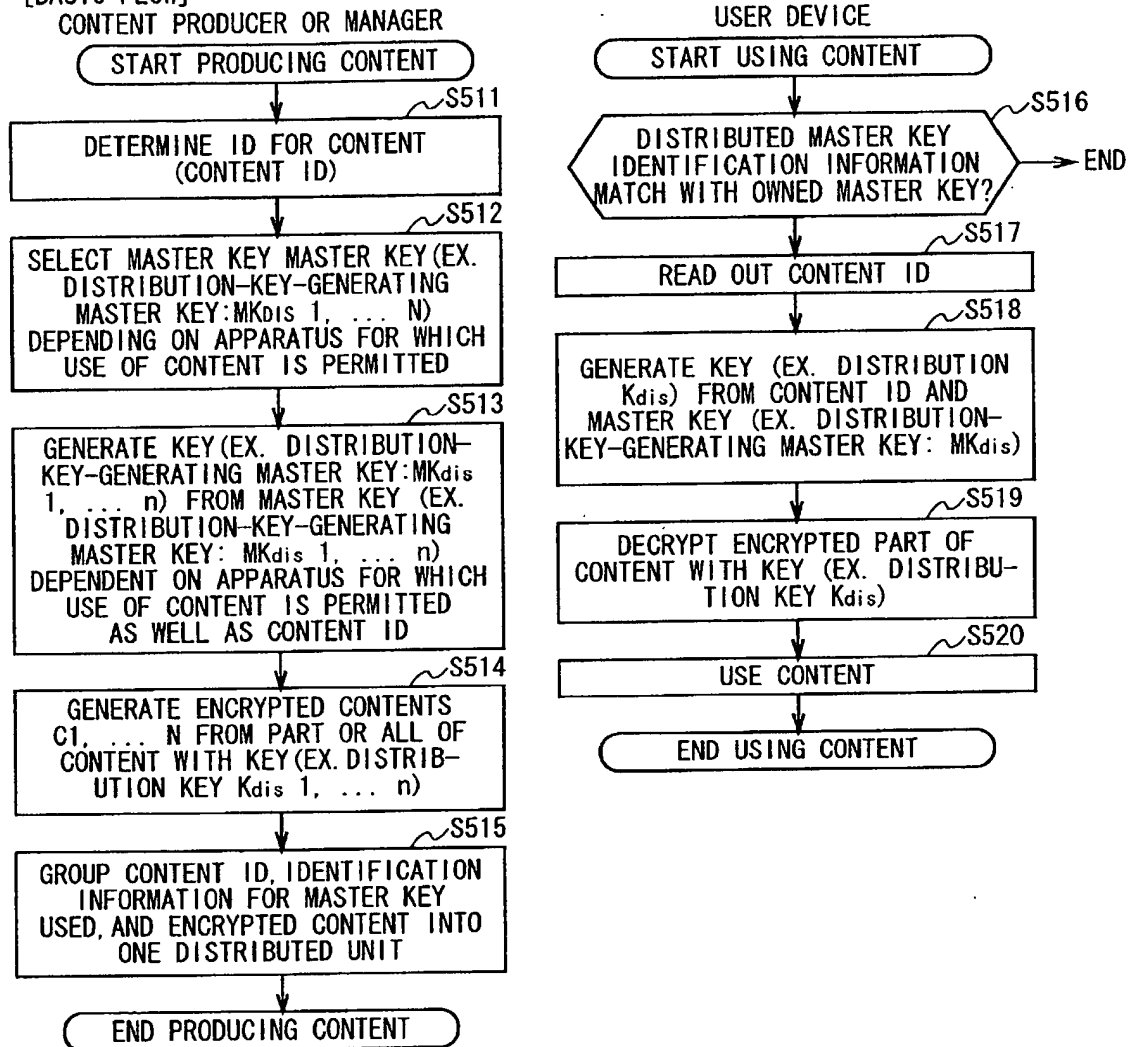


CONTENT ID

ID PROTECTED  
CONTENT

FIG. 50

METHOD FOR GENERATING INDIVIDUAL KEY FROM MASTER KEY - (2)  
[BASIC FLOW]



[KEY OWNER CONFIGURATION]  
CONTENT PRODUCER OR MANAGER

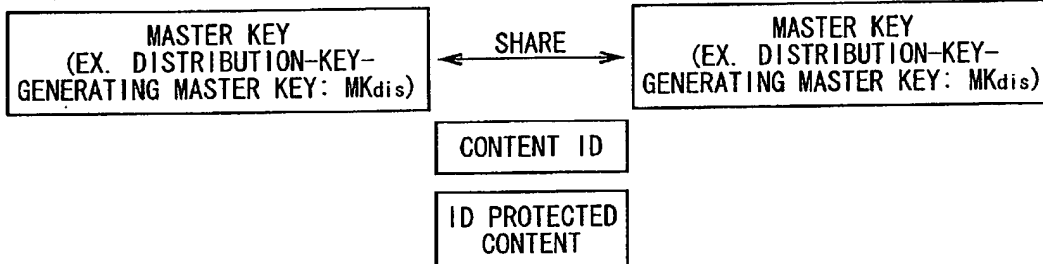


FIG. 51

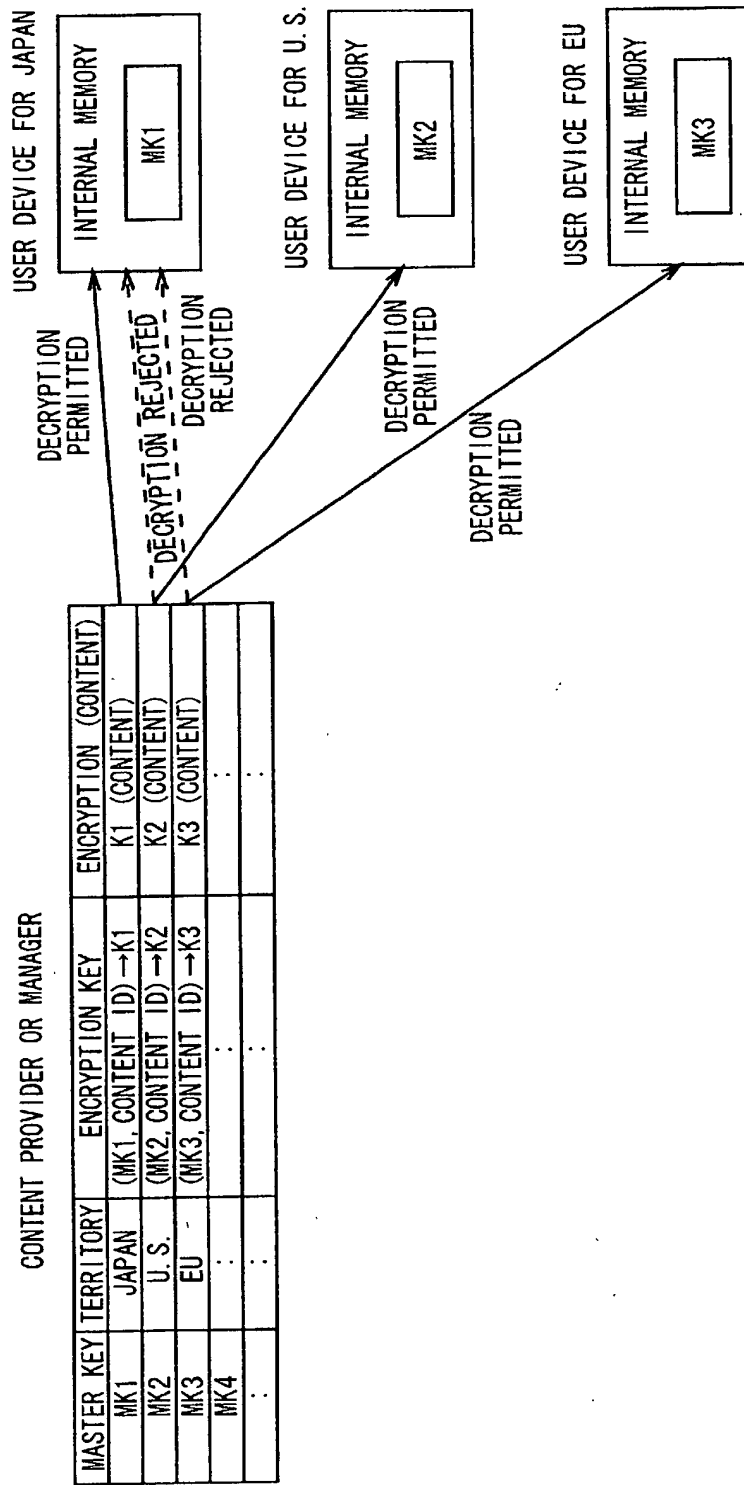
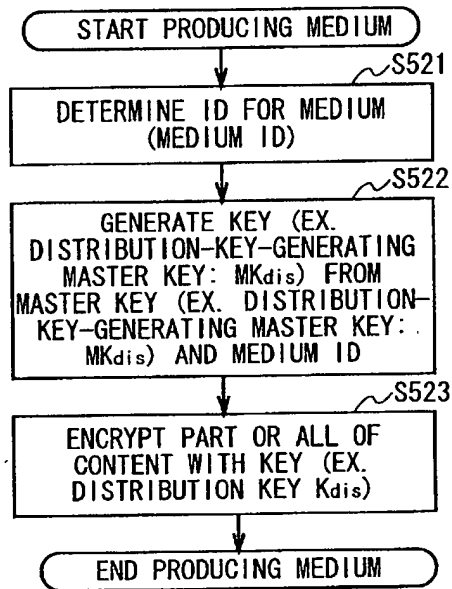


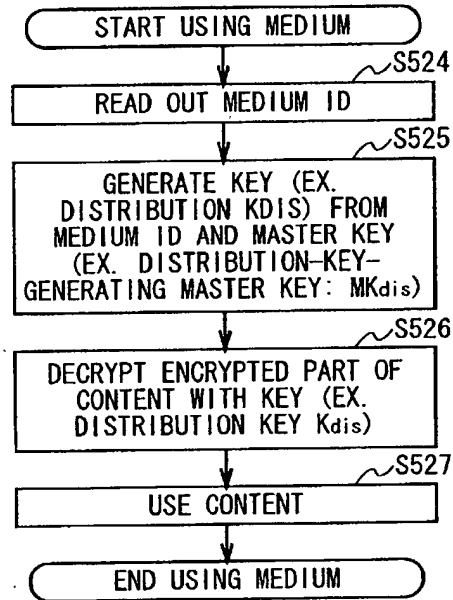
FIG. 52

METHOD FOR GENERATING INDIVIDUAL KEY FROM MASTER KEY - (3)  
[BASIC FLOW]

MEDIUM PRODUCER OR MANAGER

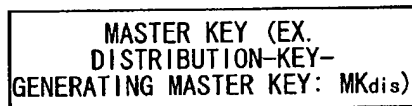


USER DEVICE



[KEY OWNER CONFIGURATION]

MEDIA CREATION OR ADMINISTRATOR



SHARE

USER DEVICE

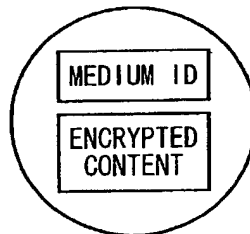
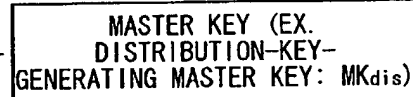
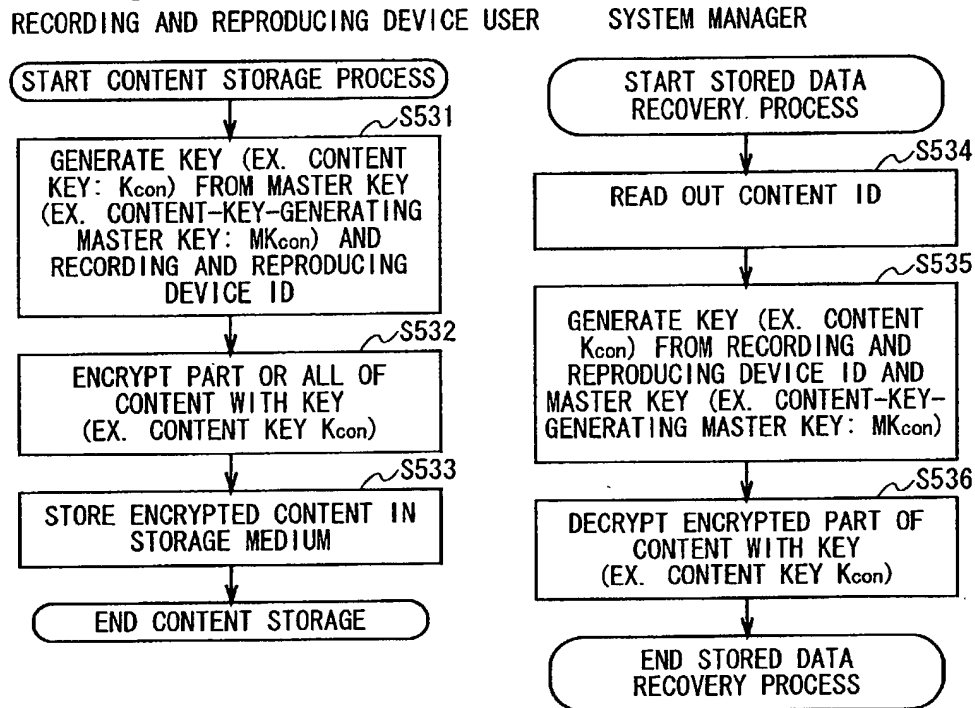


FIG. 53

METHOD FOR GENERATING INDIVIDUAL KEY FROM MASTER KEY - (4)  
 [BASIC FLOW]



[KEY OWNER CONFIGURATION]

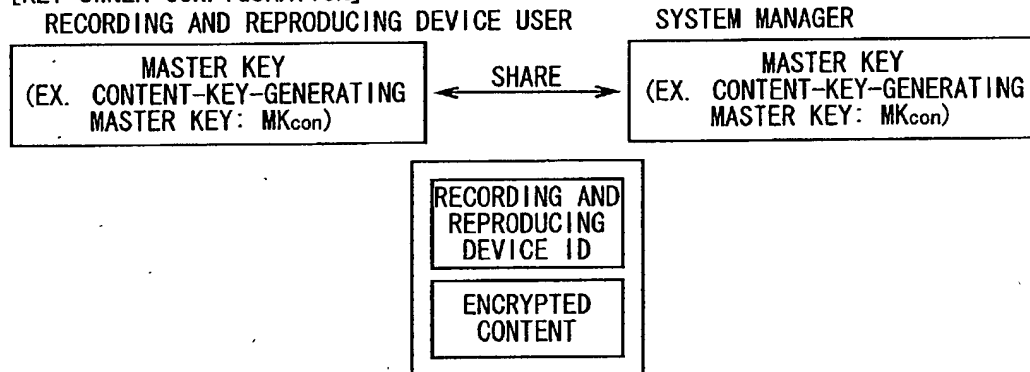
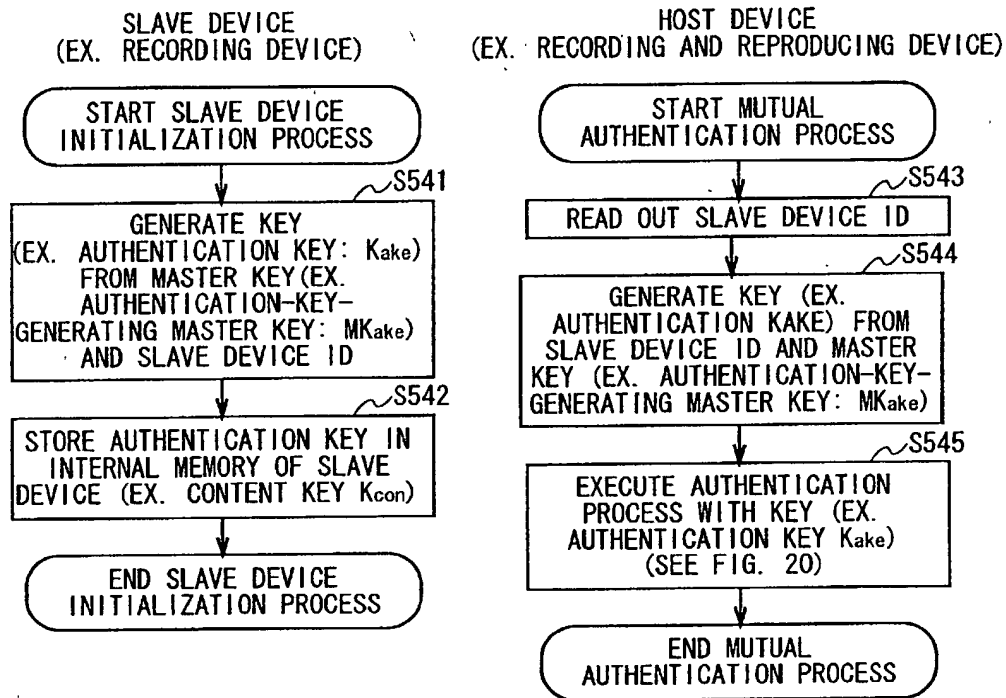


FIG. 54

METHOD FOR GENERATING INDIVIDUAL KEY FROM MASTER KEY - (5)  
[BASIC FLOW]



[KEY OWNER CONFIGURATION]

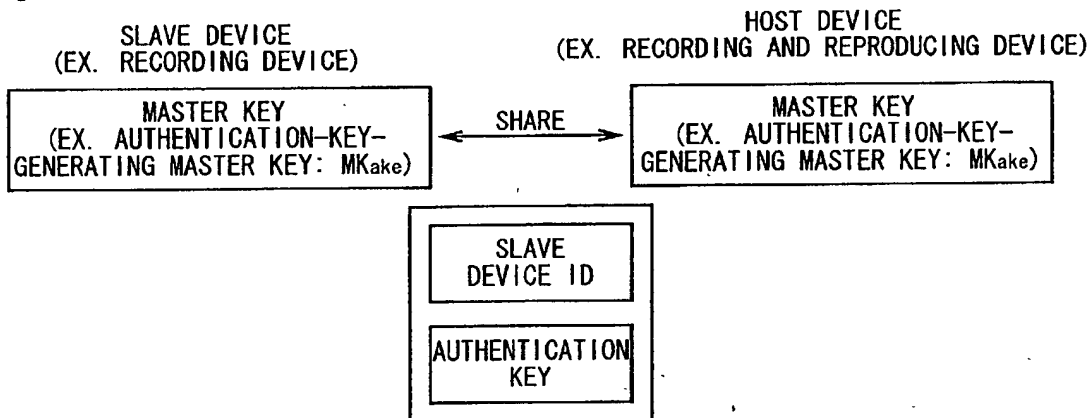


FIG. 55

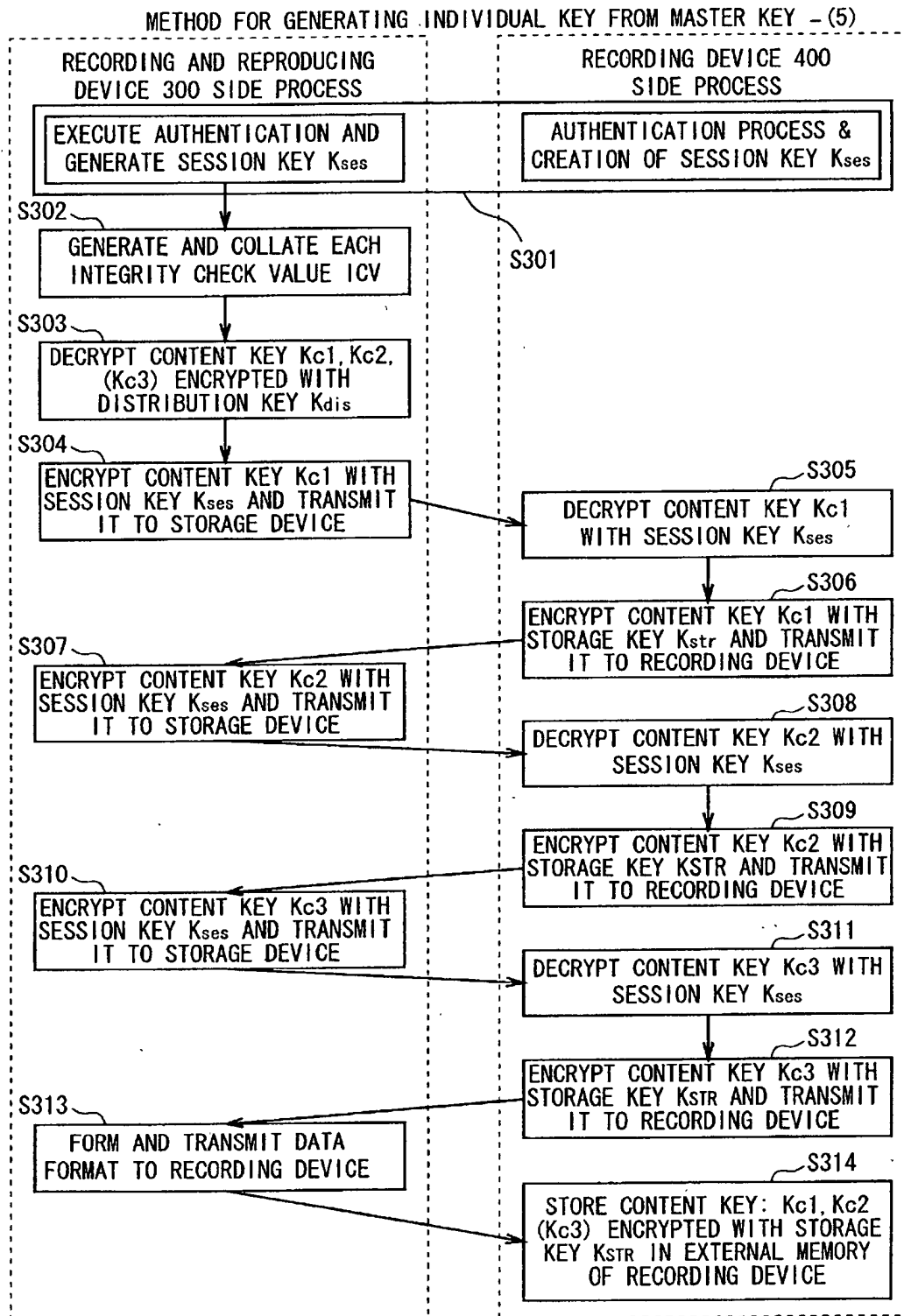


FIG. 56  
55/93

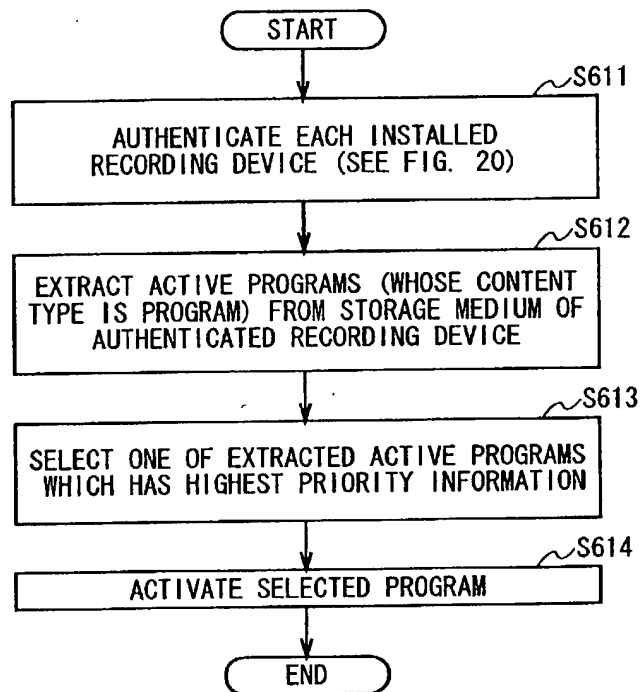


FIG. 57



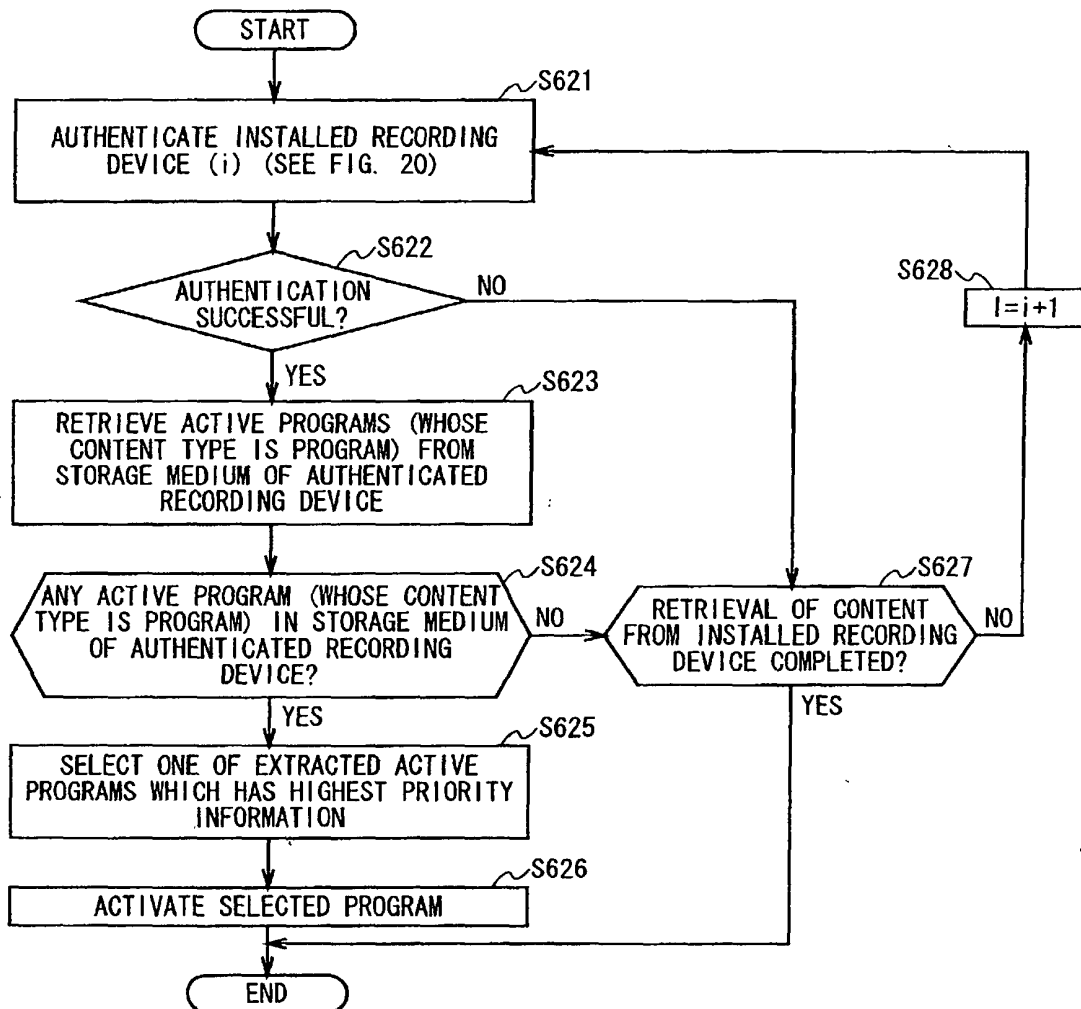


FIG. 58

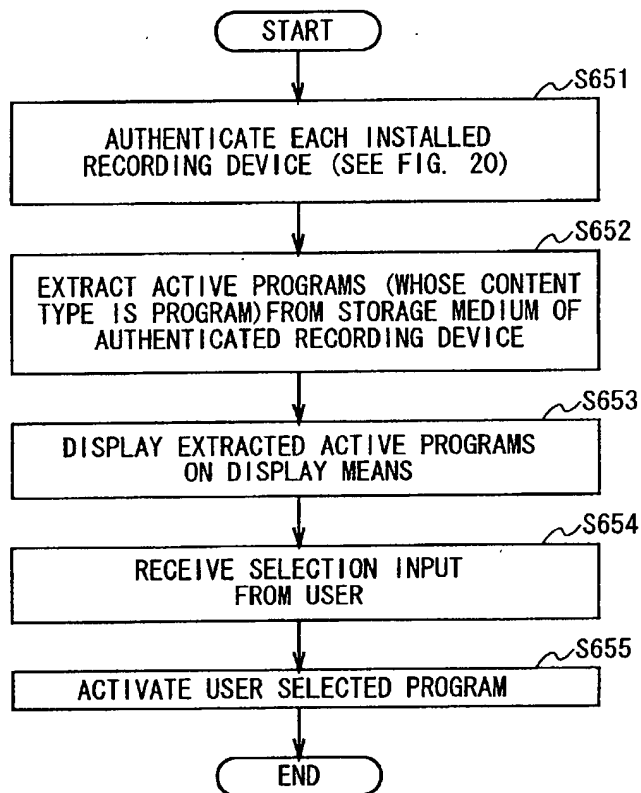


FIG. 59

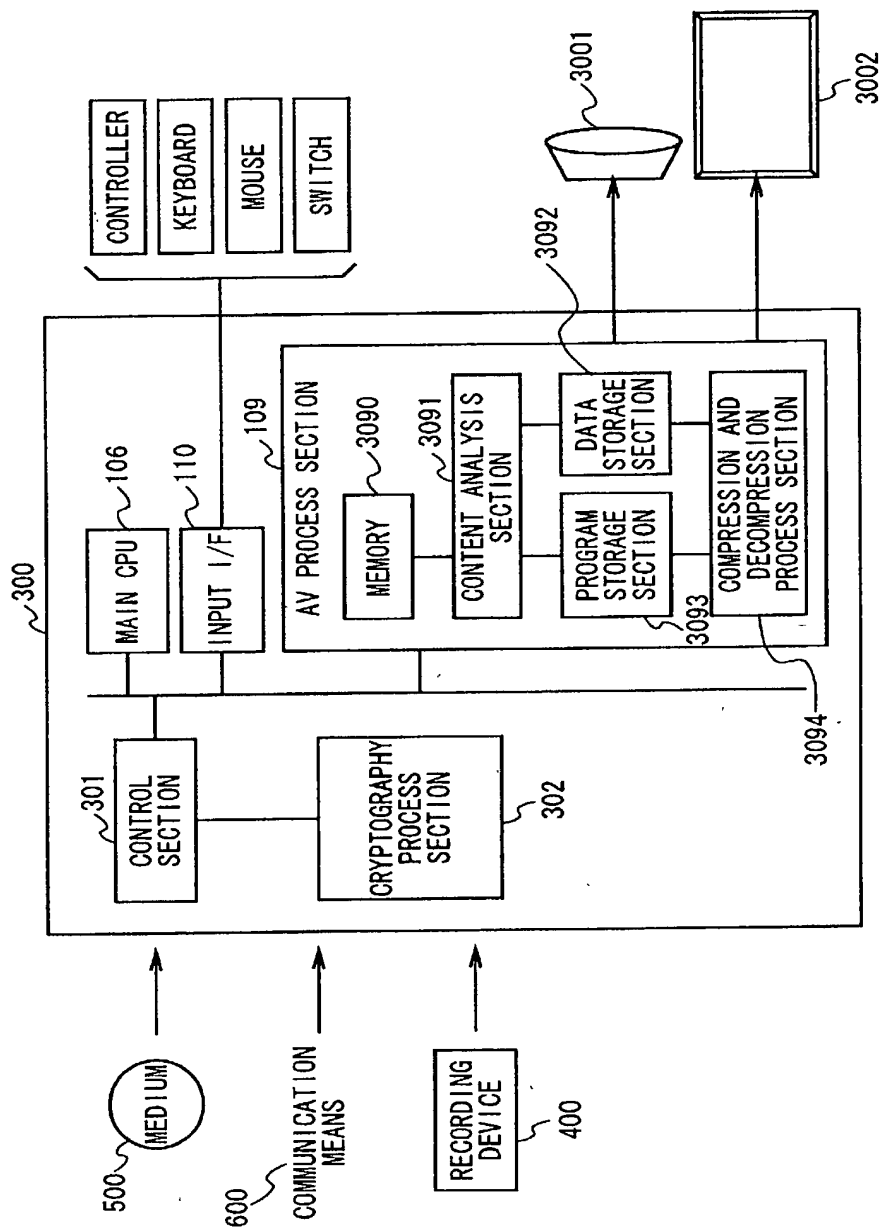


FIG. 60

EXAMPLE OF CONTENT CONFIGURATION (1)

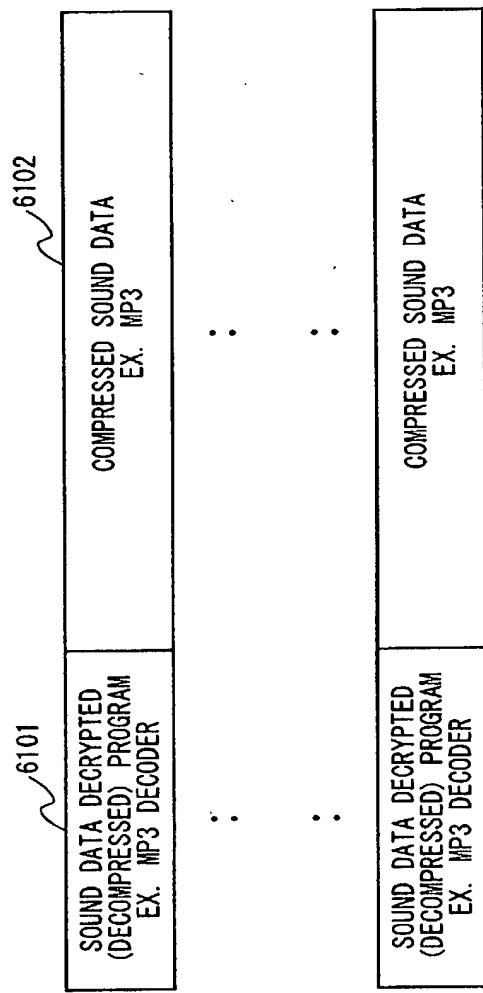


FIG. 61

09/937120

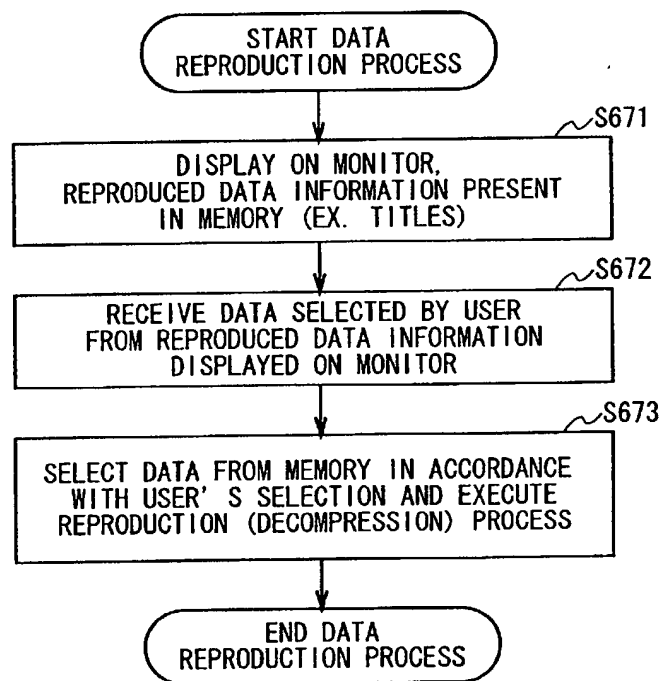


FIG. 62

EXAMPLE OF CONTENT CONFIGURATION (2)

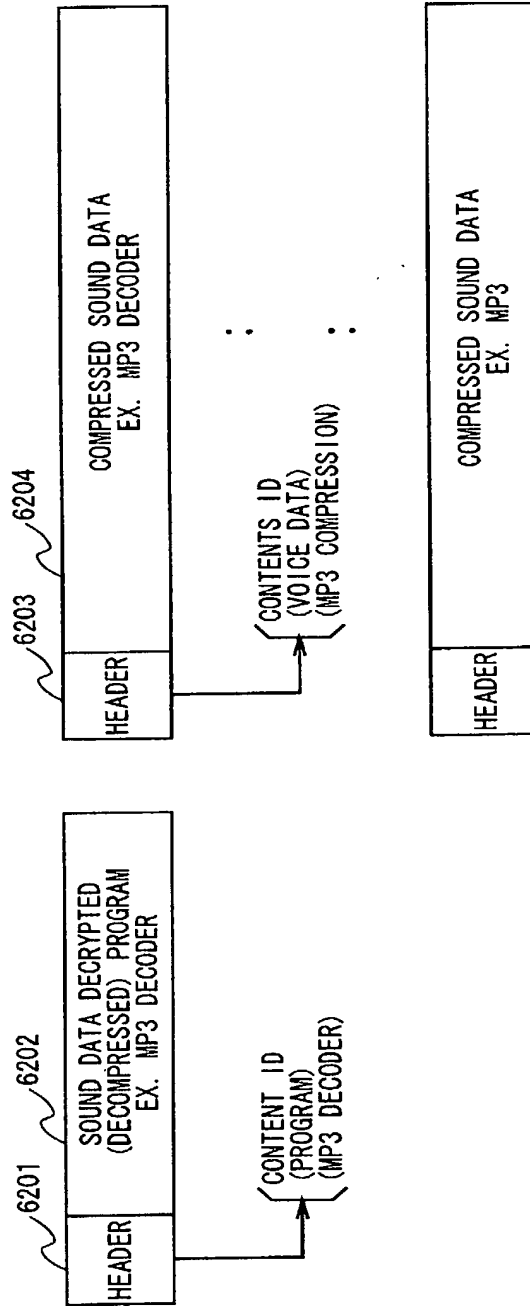


FIG. 63

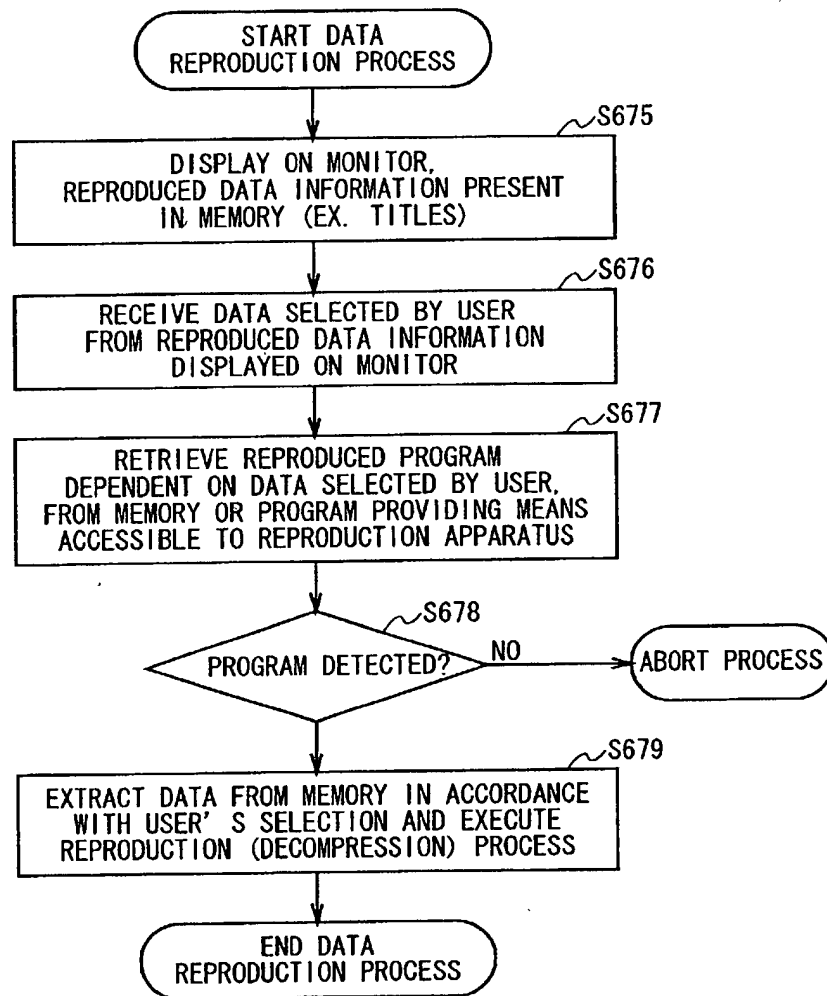


FIG. 64

EXAMPLE OF CONTENT CONFIGURATION (3)

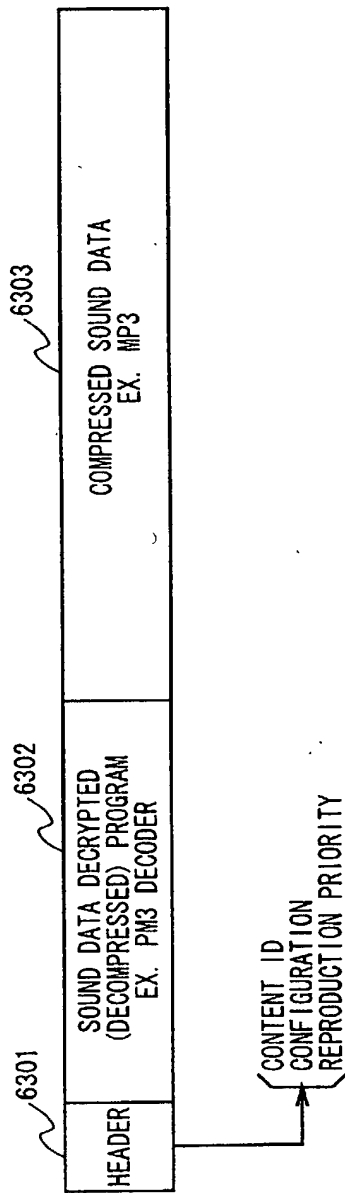


FIG. 65



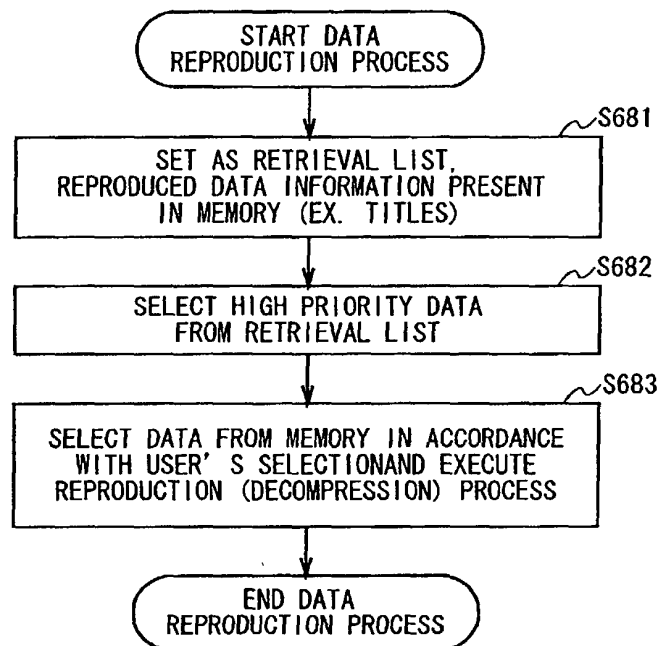


FIG. 66

EXAMPLE OF CONTENT CONFIGURATION (4)

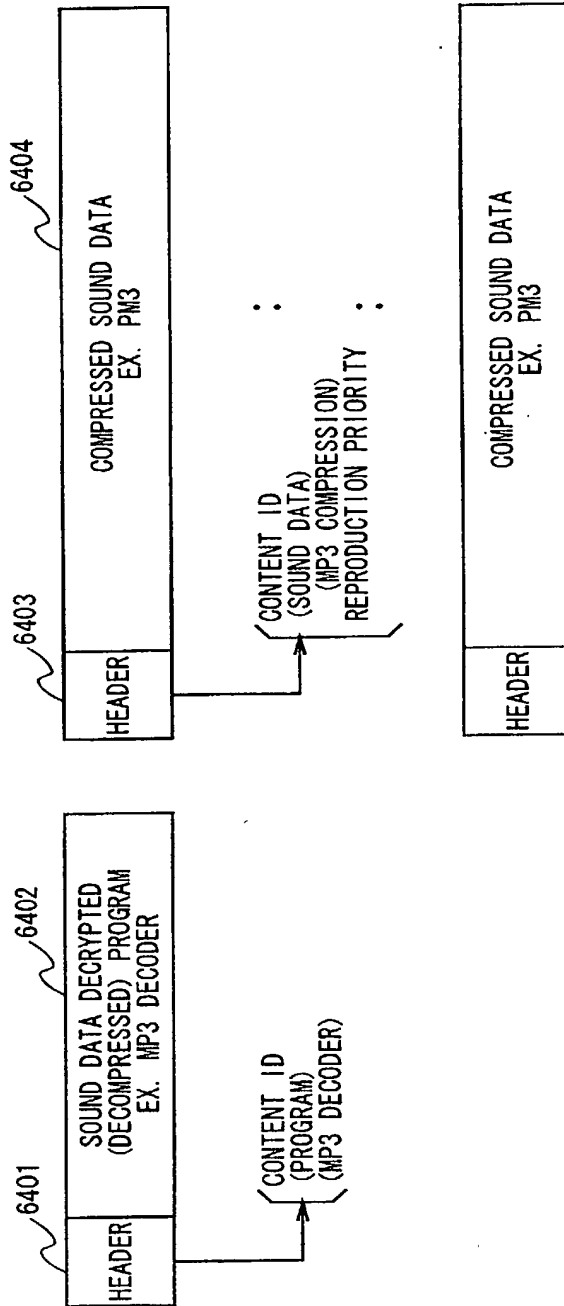


FIG. 67

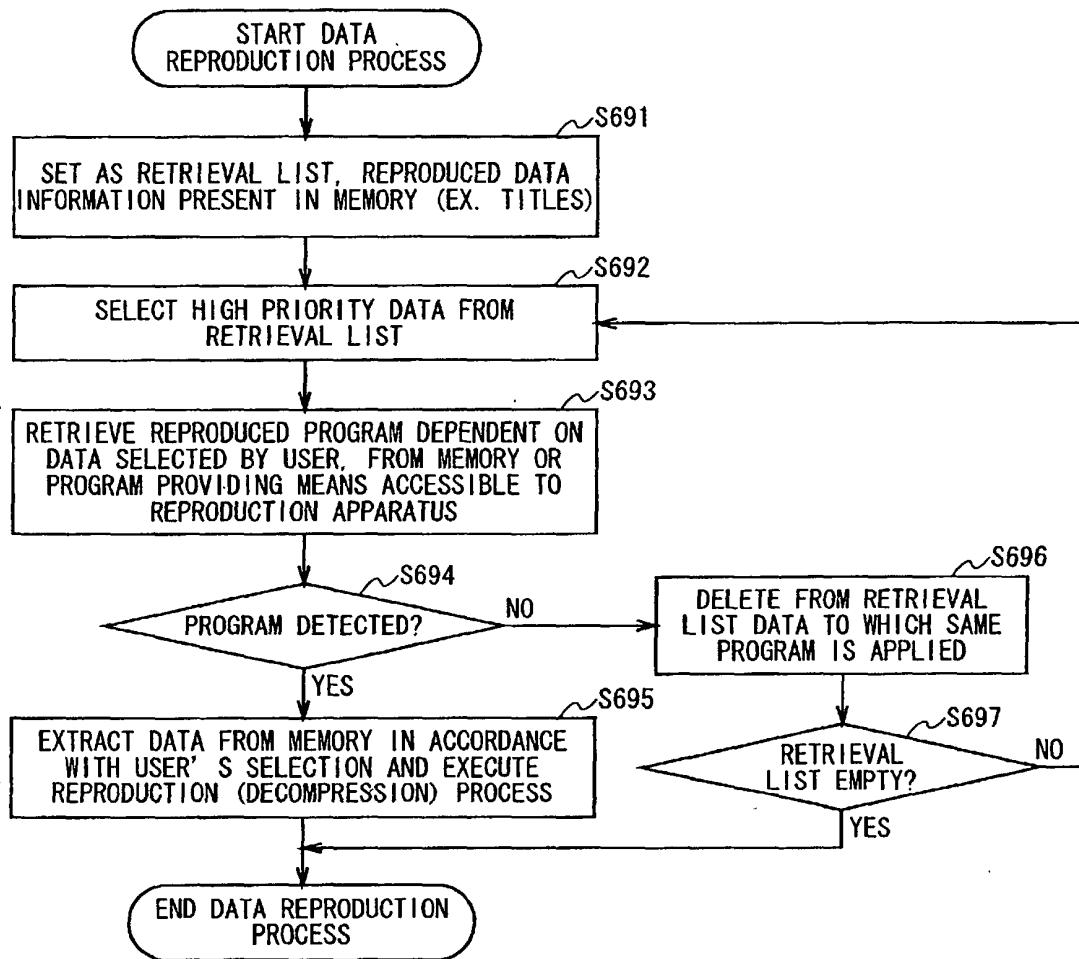
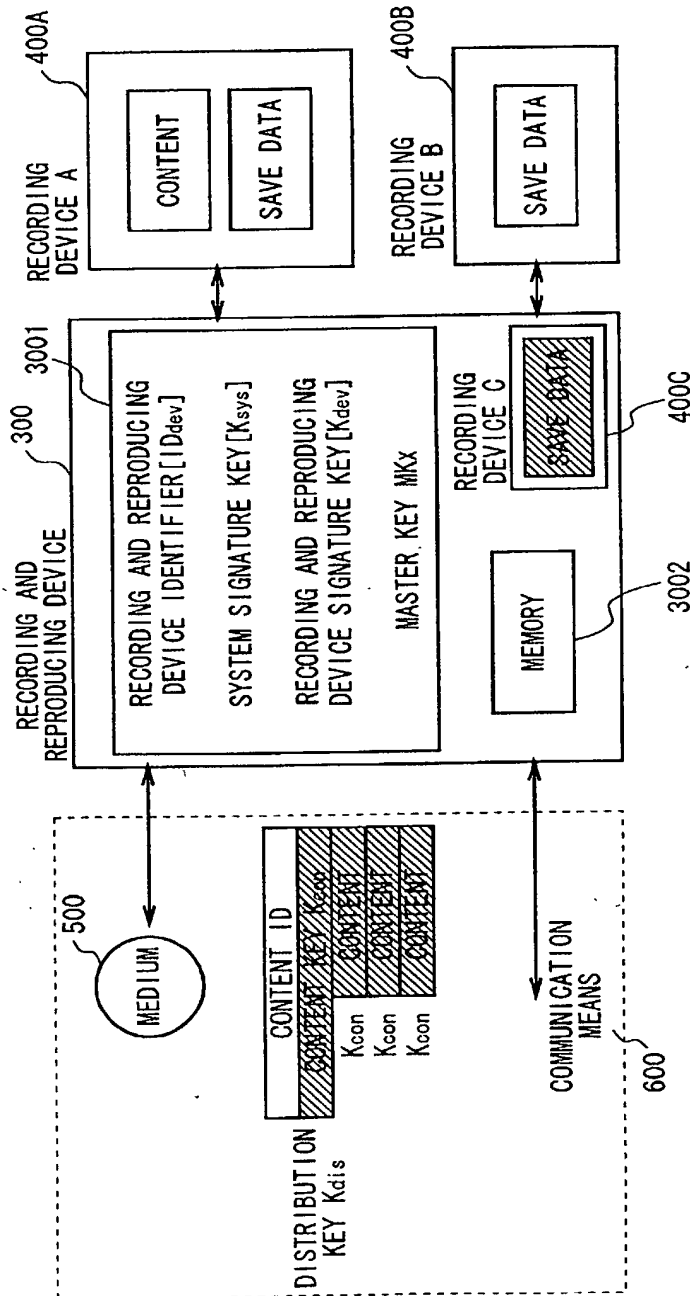


FIG. 68



SAVE DATA CRYPTOGRAPHY KEY:  $K_{sav}=K_{con}$

SAVE DATA CRYPTOGRAPHY KEY:  $K_{sav}=K_{sys}$

SAVE DATA CRYPTOGRAPHY KEY:  $K_{sav}=K_{dev}$

SAVE DATA CRYPTOGRAPHY KEY:  $K_{sav}=\text{CONTENT ID OR DES (MKx, CONTENT ID)}$

SAVE DATA CRYPTOGRAPHY KEY:  $K_{sav}=\text{RECORDING AND REPRODUCING DEVICE ID (IDdev) OR DES (MKx, RECORDING AND REPRODUCING DEVICE ID (IDdev))}$

SAVE DATA CRYPTOGRAPHY KEY:  $K_{sav}=(K_{con} \cdot K_{dev}) \text{ OR DES (MKx, } K_{con} \cdot K_{dev})$

SAVE DATA CRYPTOGRAPHY KEY:  $K_{sav}=(\text{CONTENT ID} \cdot K_{dev}) \text{ OR DES (MKx, CONTENT ID} \cdot K_{dev})$

SAVE DATA CRYPTOGRAPHY KEY:  $K_{sav}=(K_{con} \cdot \text{RECORDING AND REPRODUCING DEVICE ID}) \text{ OR DES (MKx, } K_{con} \cdot \text{RECORDING AND REPRODUCING DEVICE ID})$

SAVE DATA CRYPTOGRAPHY KEY:  $K_{sav}=(\text{CONTENT ID} \cdot \text{RECORDING AND REPRODUCING DEVICE ID})$

SAVE DATA CRYPTOGRAPHY KEY:  $K_{sav}=(\text{CONTENT ID} \cdot \text{RECORDING AND REPRODUCING DEVICE ID}) \text{ OR DES (MKx, CONTENT ID} \cdot \text{RECORDING AND REPRODUCING DEVICE ID})$

SAVE DATA CRYPTOGRAPHY KEY:  $K_{sav}=\text{PASSWORD OR DES (MKx, PASSWORD) ETC.}$

FIG. 69

## (1) EXAMPLE OF SAVE DATA STORAGE PROCESS USING CONTENT UNIQUE KEY CONTENT OR SYSTEM COMMON KEY

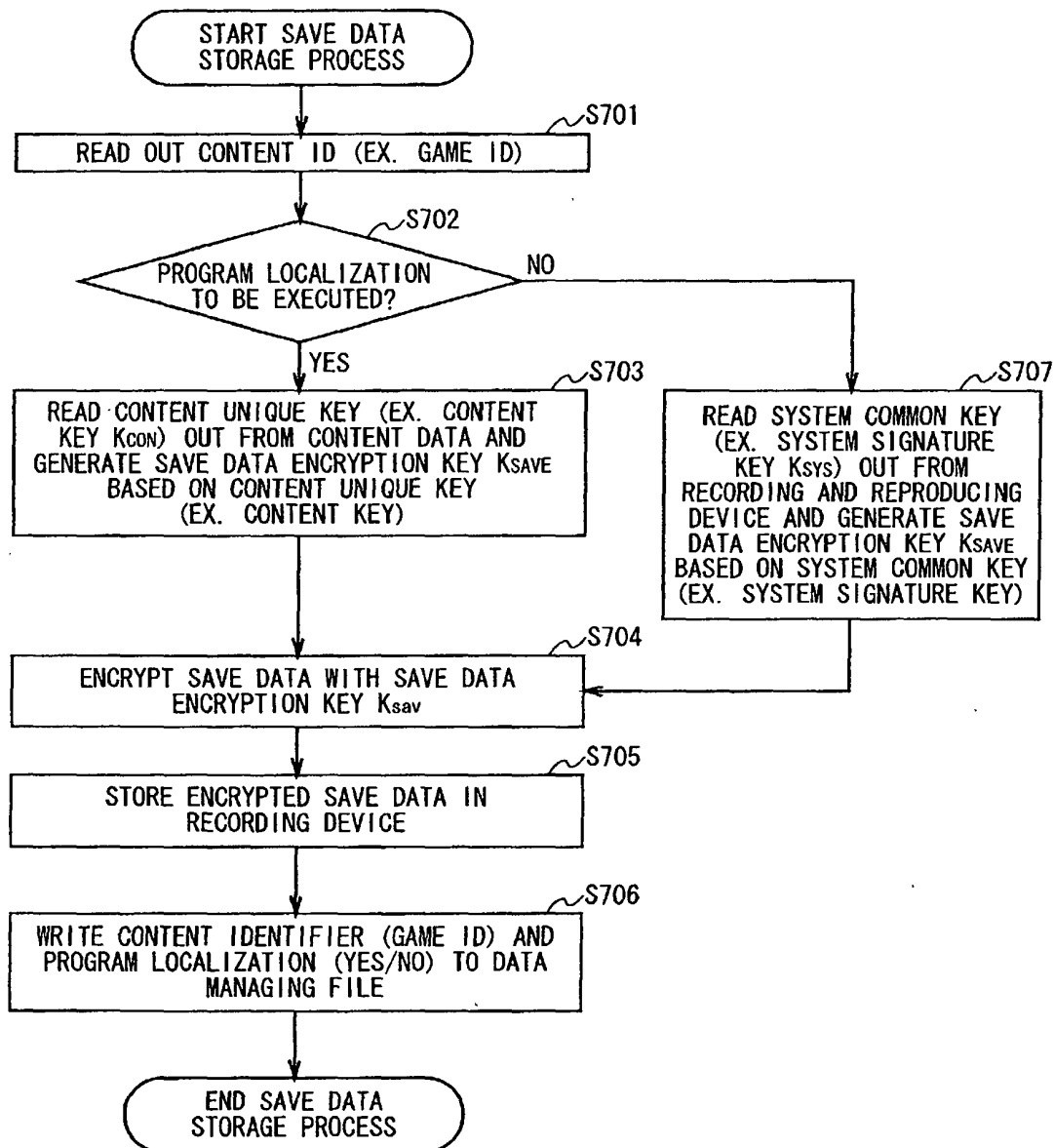


FIG. 70

# SECRET

09/937120

DATA MANAGING FILE(1)

DATA NUMBER	CONTENT ID (GAME ID)	RECORDING AND REPRODUCING DEVICE ID (IDDEV)	PROGRAM LOCALIZATION
1	12345678...	56789012...	YES
2	ABCDEF12...	09876543...	YES
3	12245678...	58834762...	NO
⋮	⋮	⋮	⋮

FIG. 71

## (2) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING CONTENT UNIQUE KEY OR SYSTEM COMMON KEY

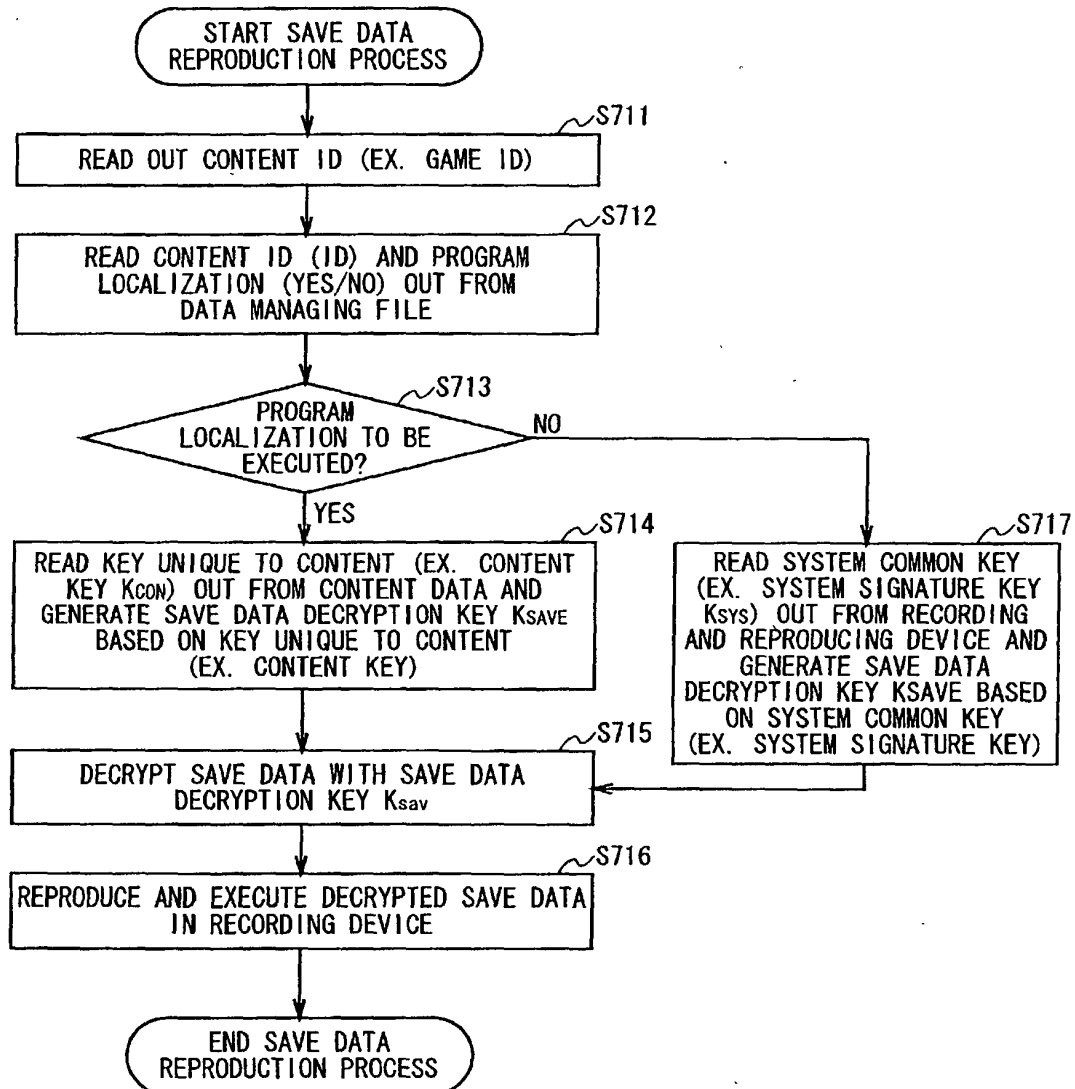


FIG. 72

## (3) EXAMPLE OF SAVE DATA STORAGE PROCESS USING CONTENT ID OR SYSTEM COMMON KEY

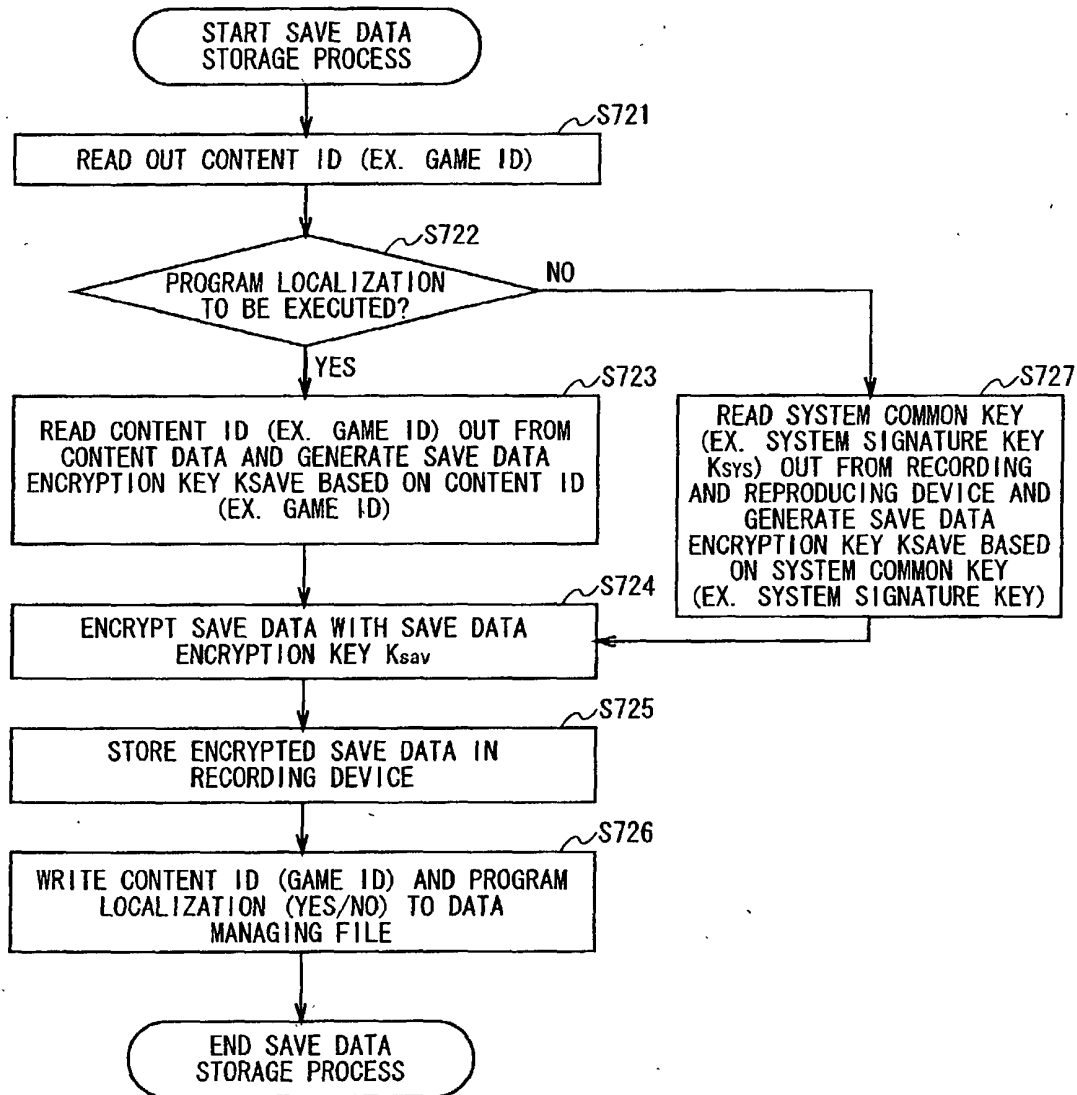


FIG. 73



(4) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING CONTENT ID OR SYSTEM COMMON KEY

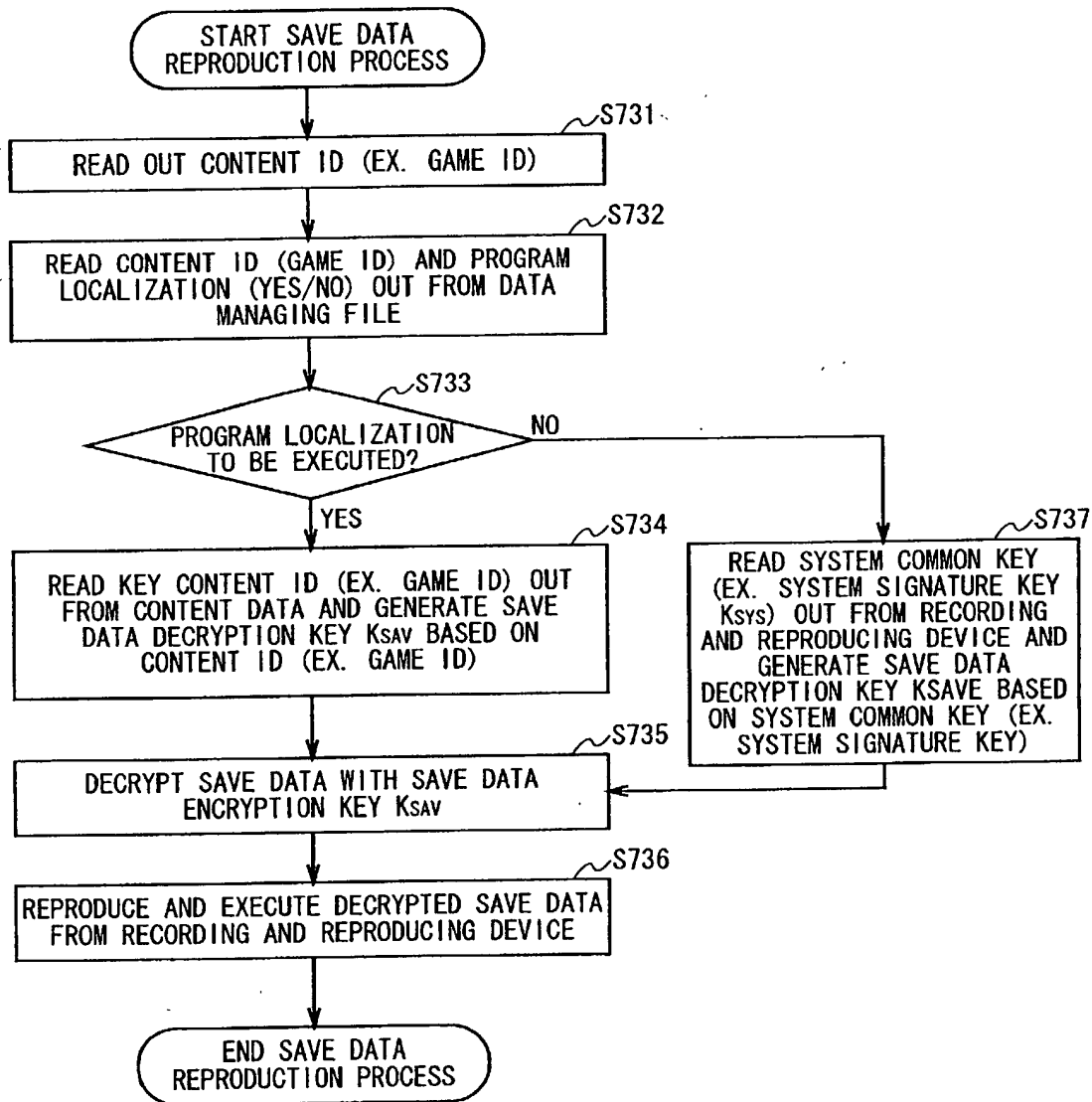


FIG. 74

(5) EXAMPLE OF SAVE DATA STORAGE PROCESS USING RECORDING AND REPRODUCING DEVICE UNIQUE KEY OR SYSTEM COMMON KEY

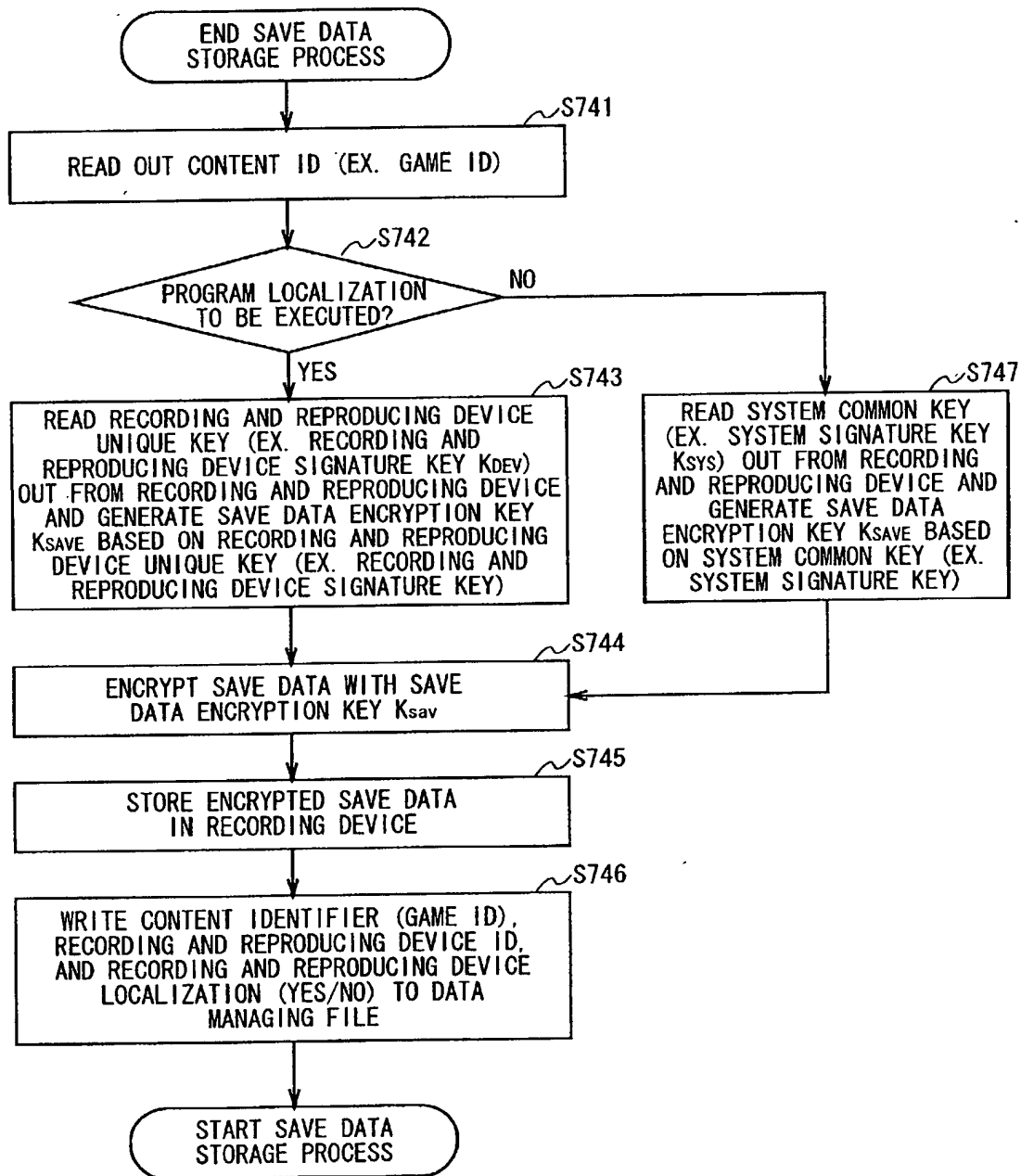


FIG. 75

DATA MANAGING FILE (2)

DATA NUMBER	CONTENT ID (GAME ID)	RECORDING AND REPRODUCING DEVICE ID (IDdev)	PROGRAM LOCALIZATION
1	12345678...	56789012...	NO
2	ABCDEF12...	09876543...	YES
3	12245678...	58834762...	YES
⋮	⋮	⋮	⋮

FIG. 76

## (6) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING RECORDING AND REPRODUCING DEVICE UNIQUE KEY OR SYSTEM COMMON KEY

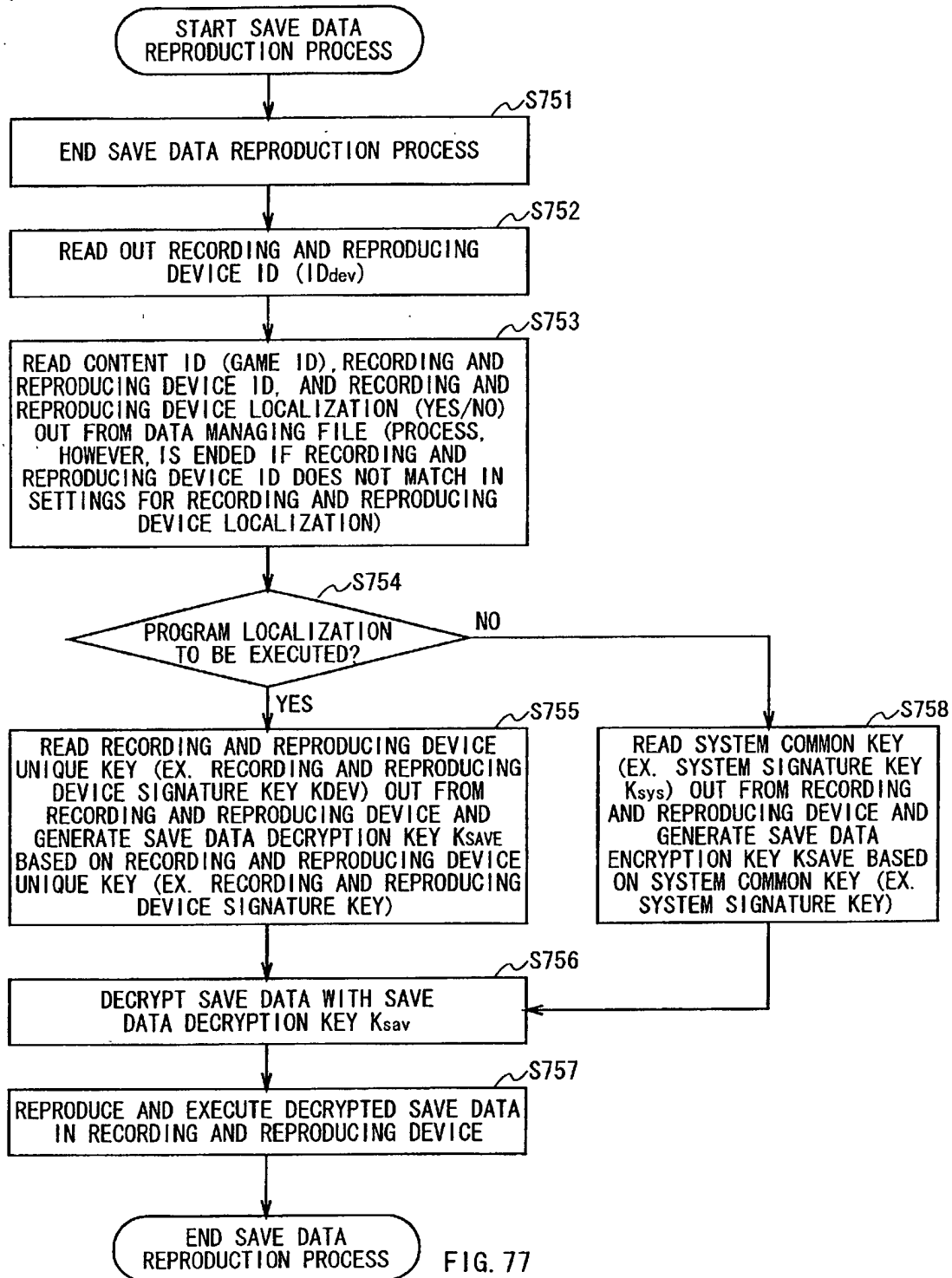


FIG. 77

## (7) EXAMPLE OF SAVE DATA STORAGE PROCESS USING RECORDING AND REPRODUCING DEVICE ID OR SYSTEM COMMON KEY

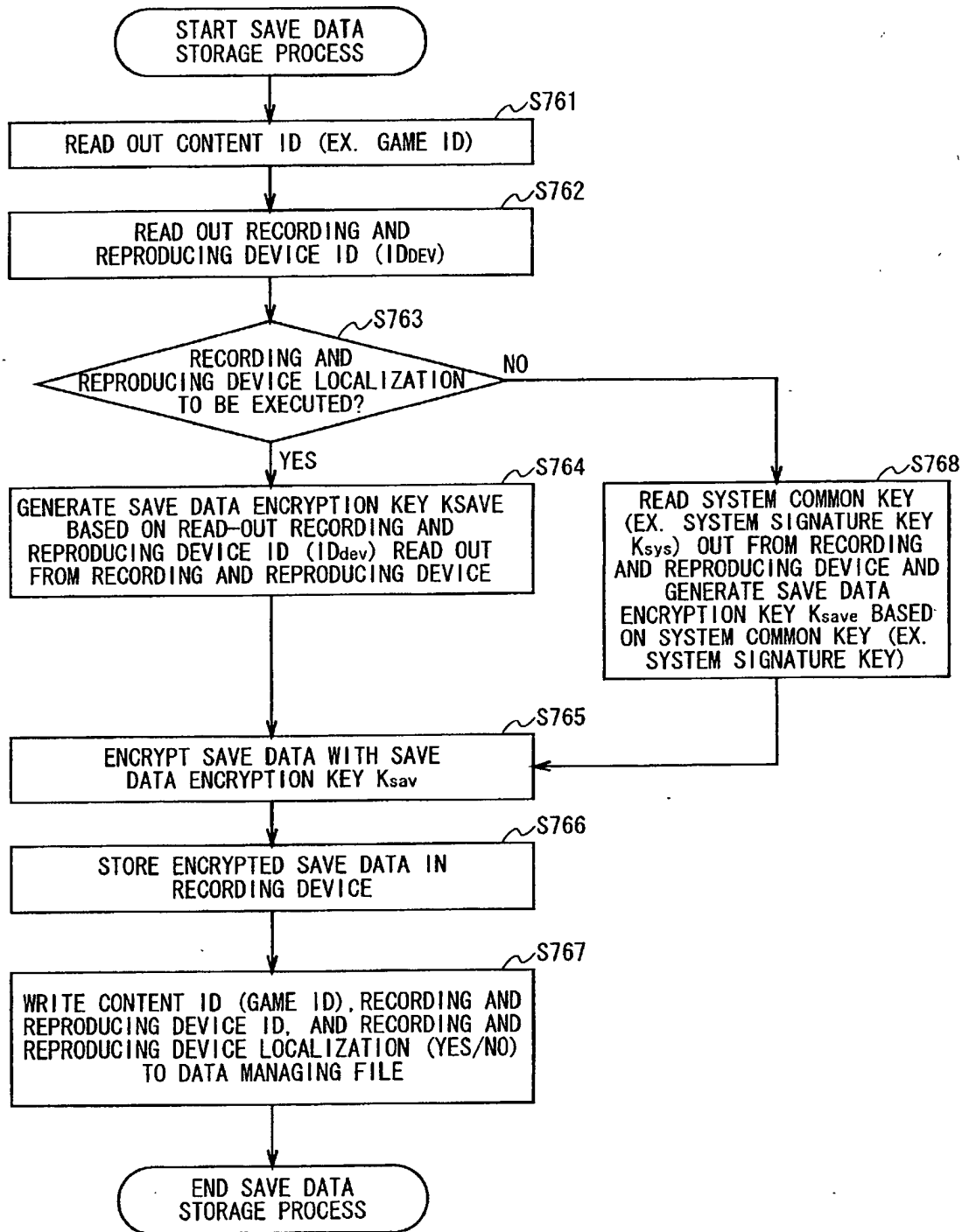


FIG. 78

## (8) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING RECORDING AND REPRODUCING DEVICE ID OR SYSTEM COMMON KEY

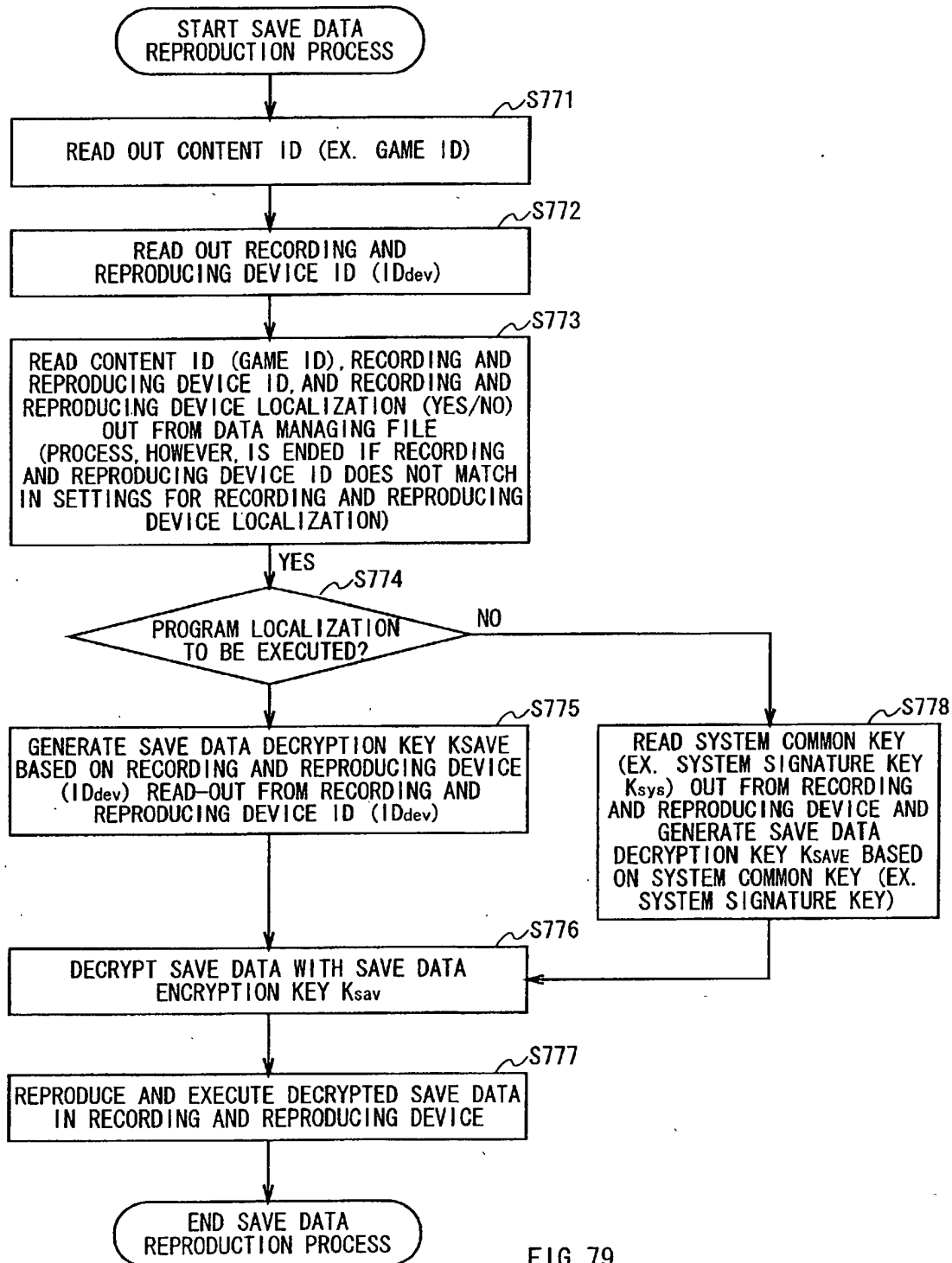
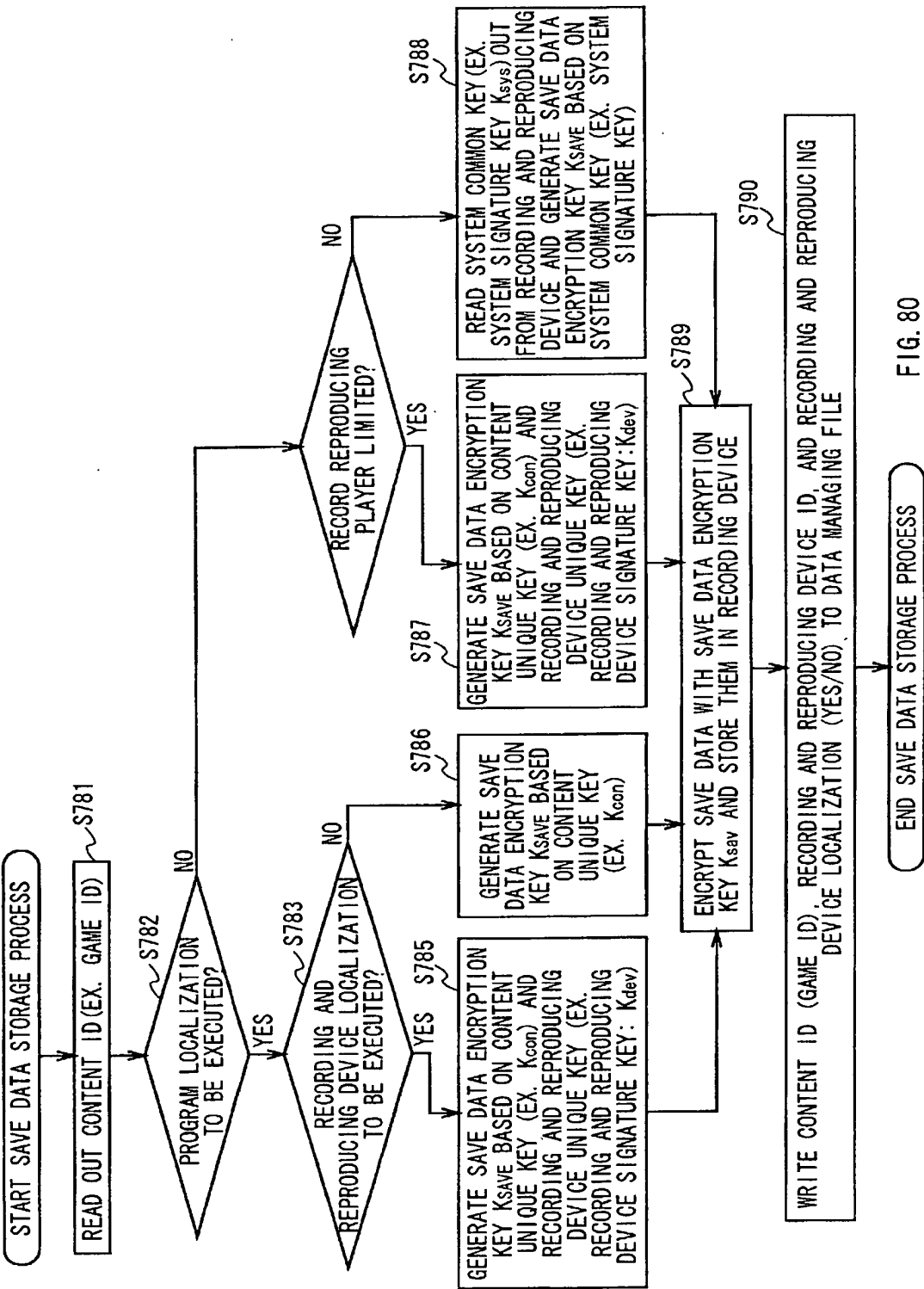


FIG. 79

(9) EXAMPLE OF SAVE DATA STORAGE PROCESS USING CONTENT UNIQUE KEY, RECORDING AND REPRODUCING DEVICE UNIQUE KEY, OR SYSTEM COMMON KEY



DATA MANAGING FILE (3)

DATA NUMBER	CONTENT ID (GAME ID)	RECORDING AND REPRODUCING DEVICE ID (ID <sub>dev</sub> )	PROGRAM LOCALIZATION	RECORDING AND REPRODUCING DEVICE LOCALIZATION
1	123455678...	56789012...	YES	NO
2	ABCDEF12...	09876543...	YES	YES
3	1122457678	58834762...	NO	YES
•	•	•	•	•
•	•	•	•	•

FIG. 81



(10) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING CONTENT UNIQUE KEY, RECORDING AND REPRODUCING DEVICE UNIQUE KEY, OR SYSTEM COMMON KEY

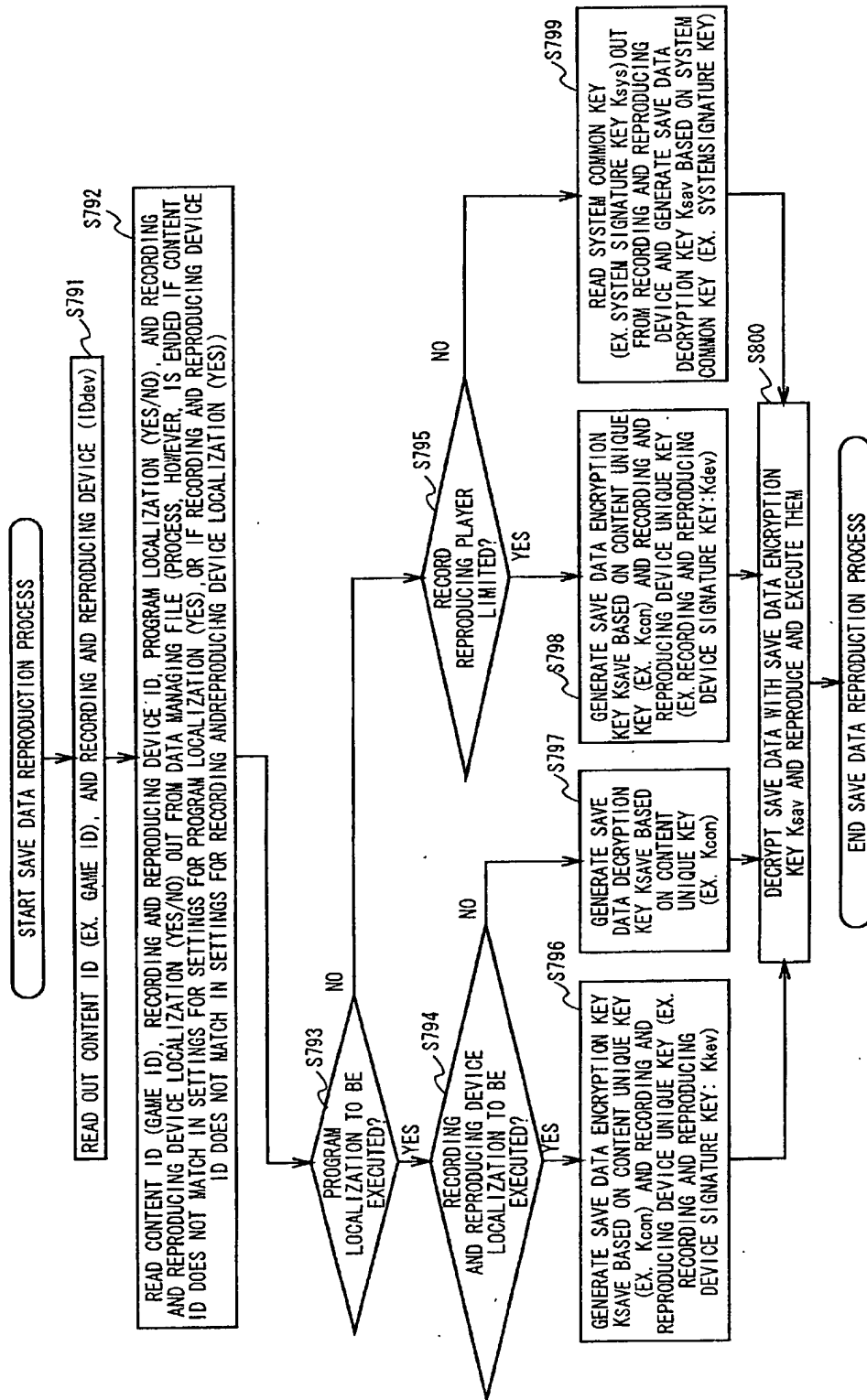


FIG. 82

## (11) EXAMPLE OF SAVE DATA STORAGE PROCESS USING USER PASSWORD OR SYSTEM COMMON KEY

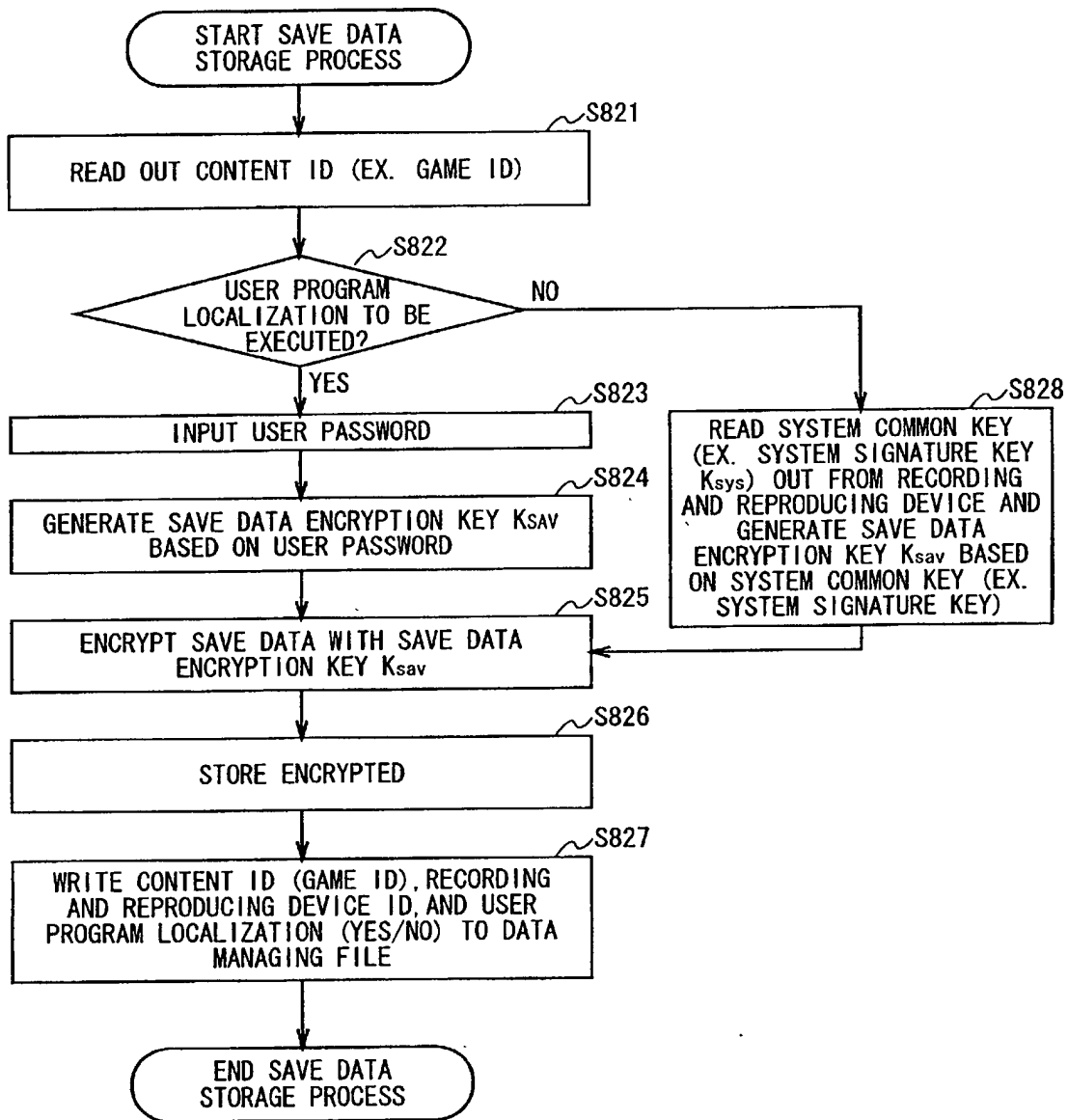


FIG. 83

TOTAL: 024560

DATA MANAGING FILE(4)

DATA NUMBER	CONTENT ID (GAME ID)	RECORDING AND REPRODUCING DEVICE ID (ID <sub>dev</sub> )	USER PROGRAM LOCALIZATION
1	123455678...	56789012...	YES
2	ABCDEF12...	09876543...	YES
3	1122457678	58834762...	NO
•	•	•	•
•	•	•	•

FIG. 84

## (12) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING USER PASSWORD OR SYSTEM COMMON KEY

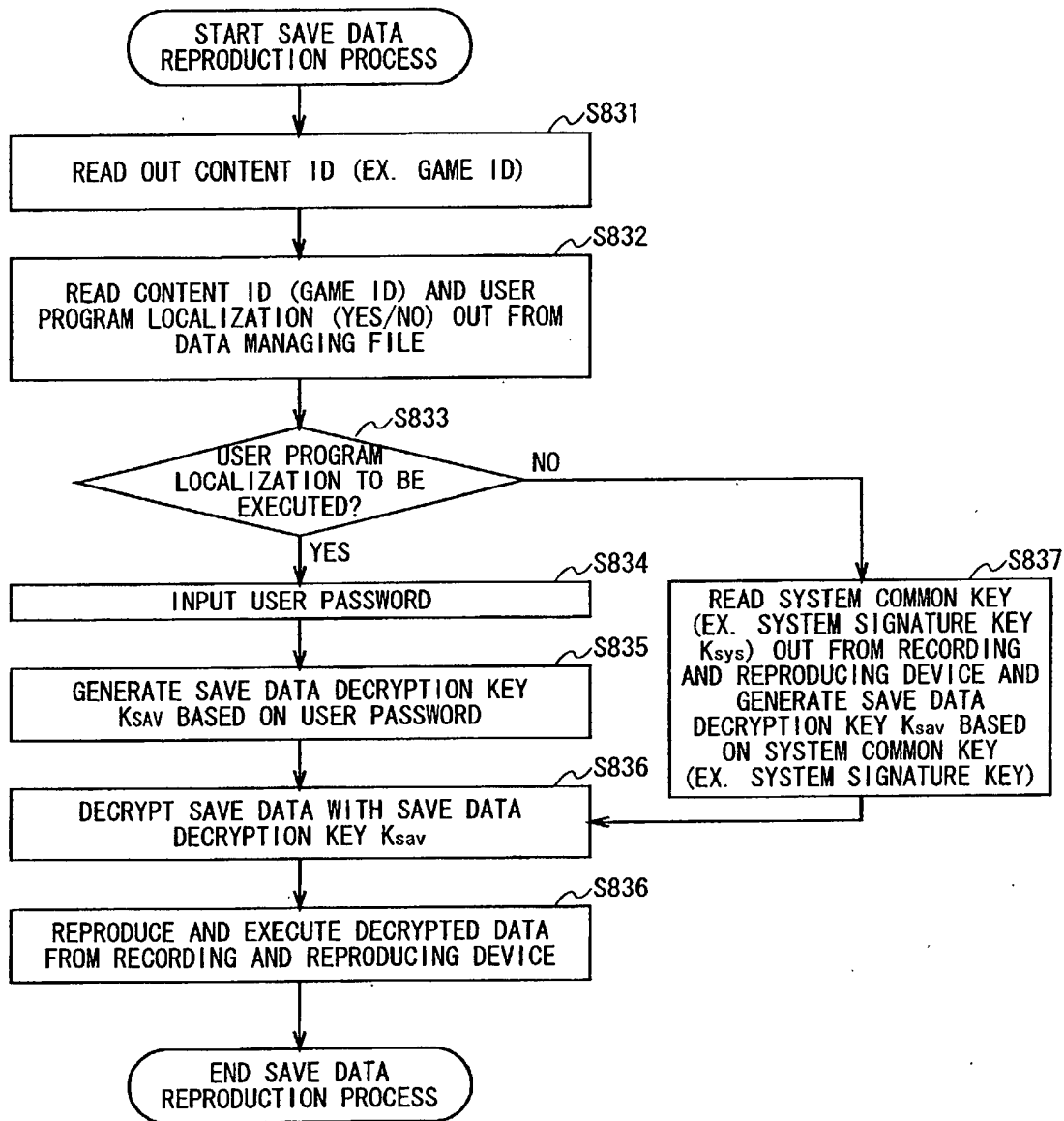


FIG. 85

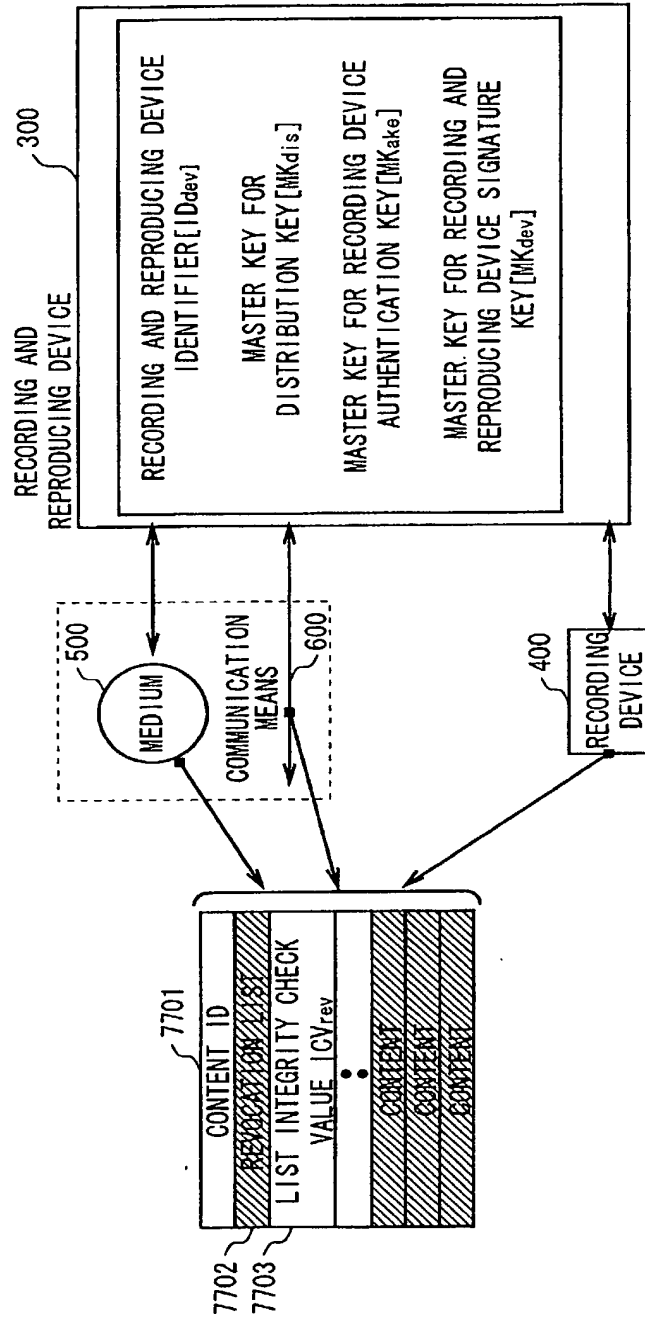


FIG. 86

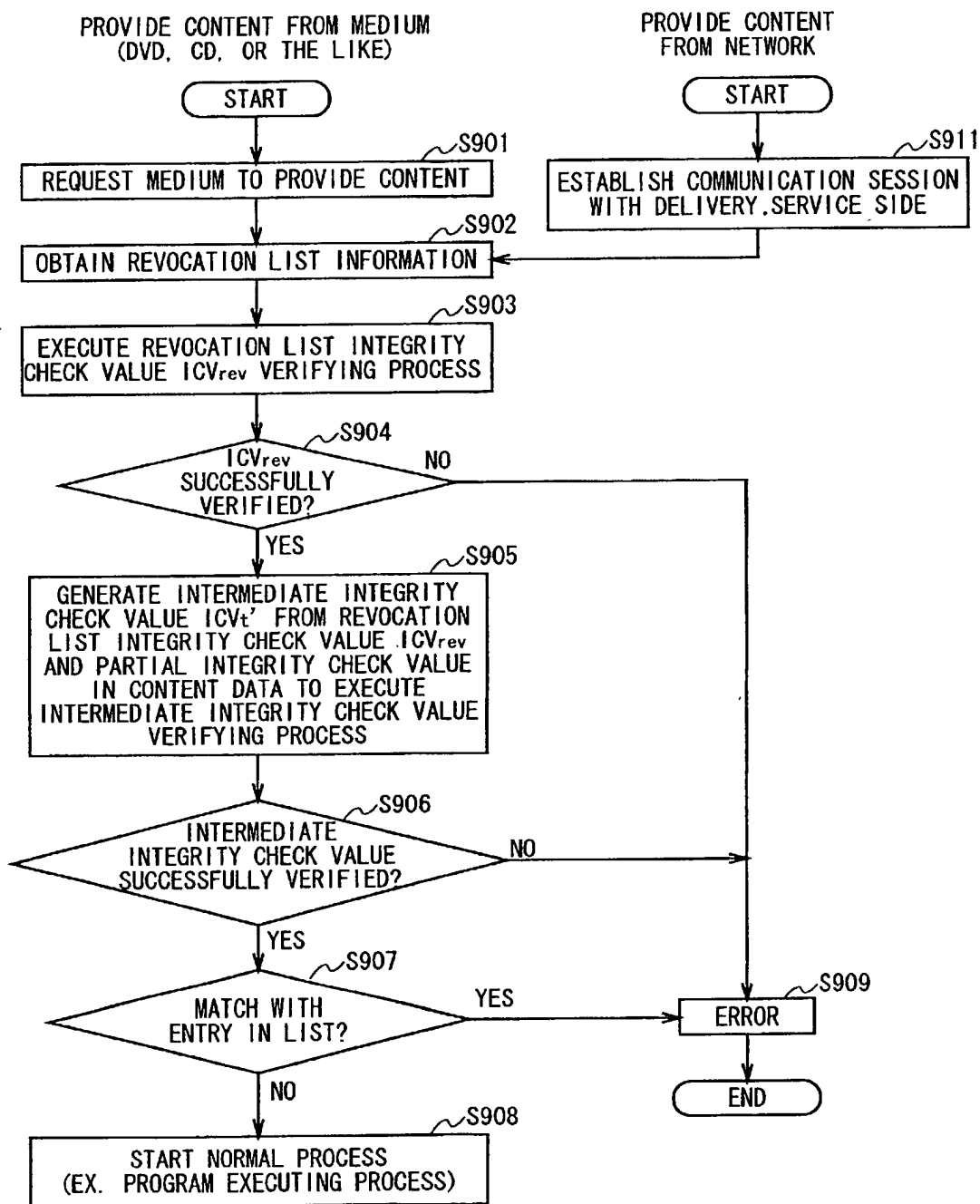


FIG. 87

PROVIDE CONTENT FROM RECORDING  
DEVICE (MEMORY CARD OR THE LIKE)

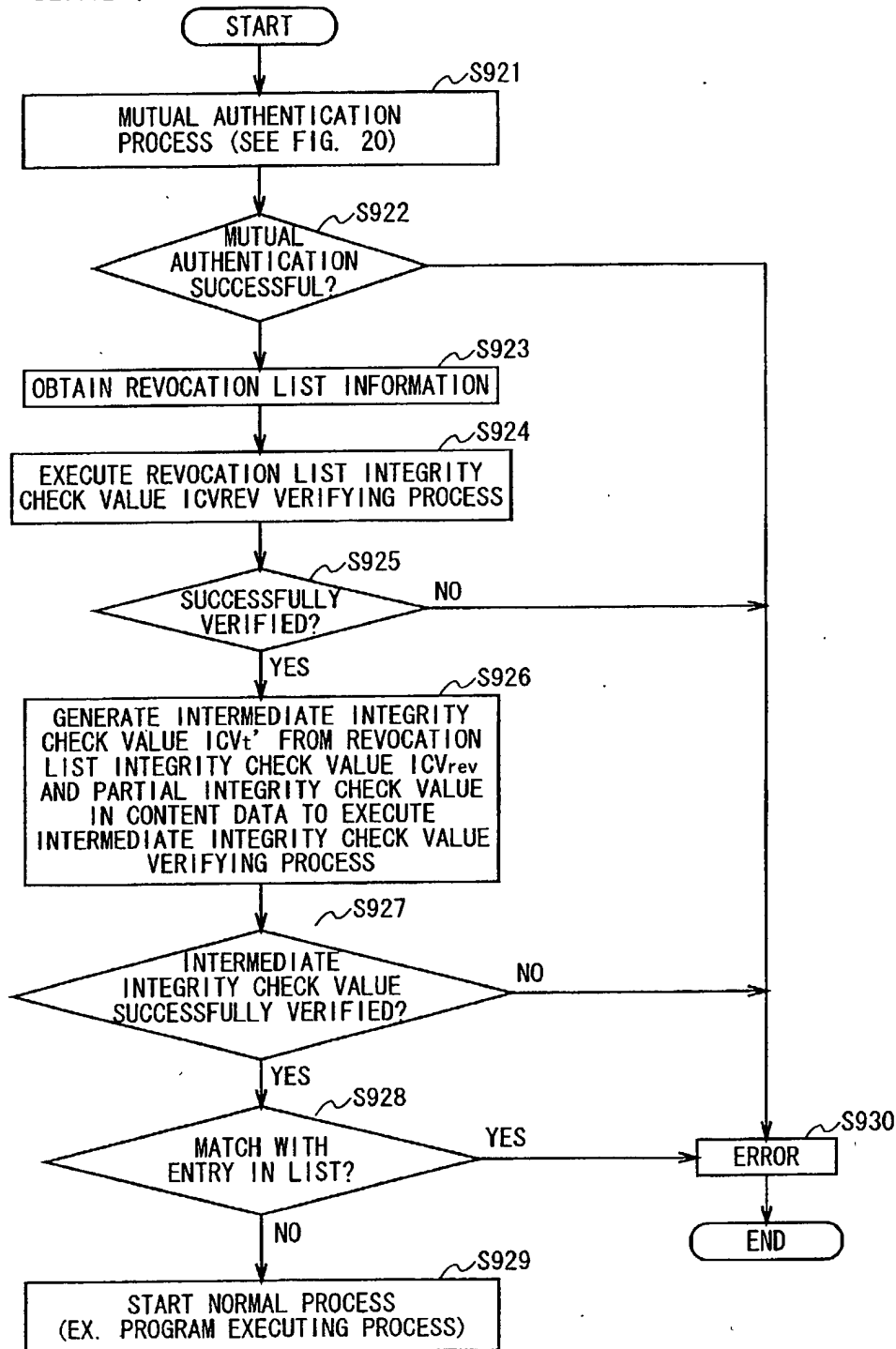


FIG. 88  
87/93

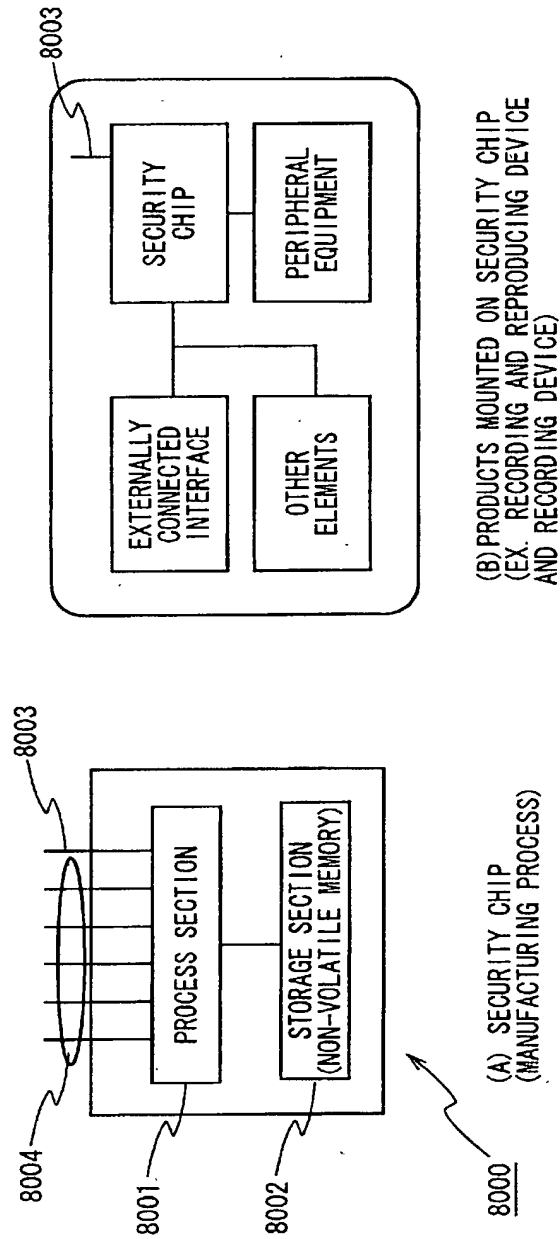


FIG. 89



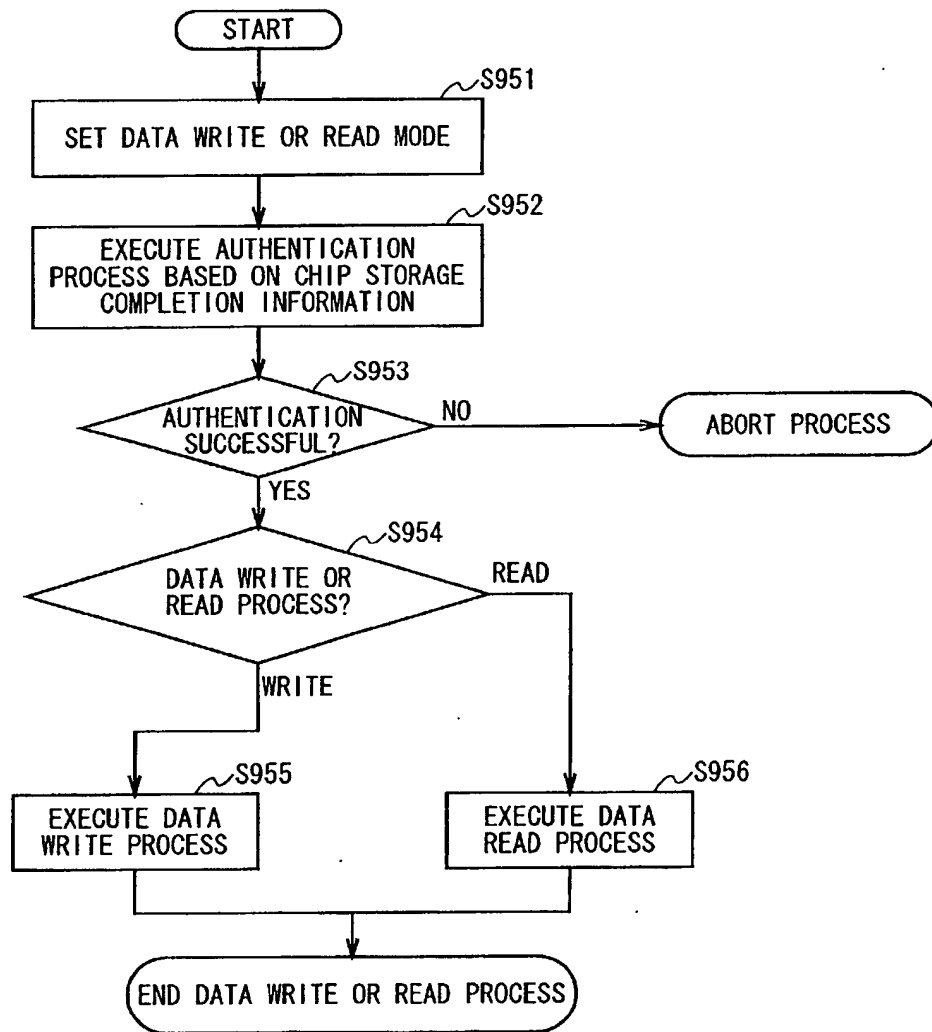
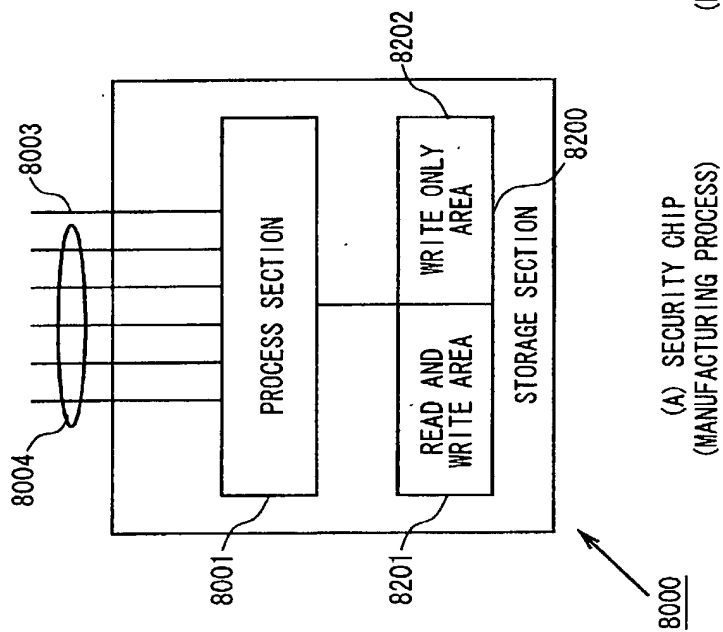
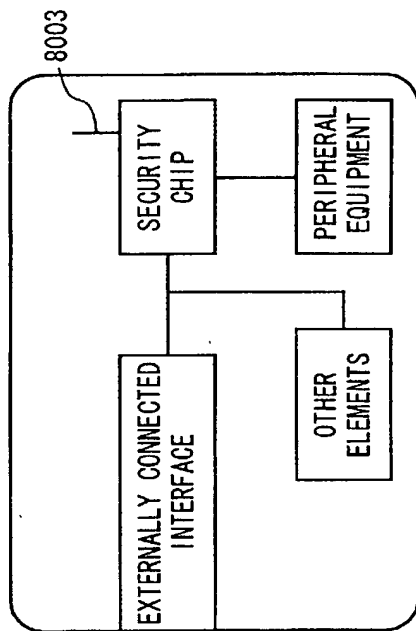
SECURITY CHIP  
MANUFACTURING PROCESS FLOW

FIG. 90



(A) SECURITY CHIP  
(MANUFACTURING PROCESS)



(B) PRODUCTS MOUNTED ON SECURITY CHIP  
(EX. RECORDING AND REPRODUCING DEVICE AND RECORDING DEVICE)

FIG. 91

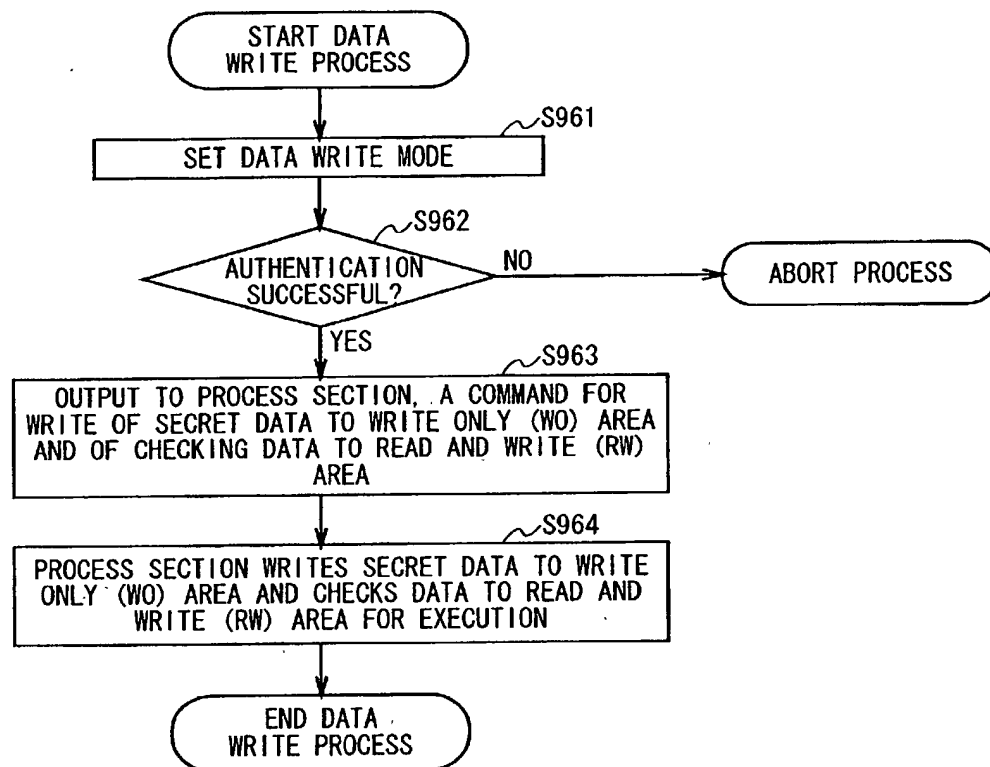


FIG. 92

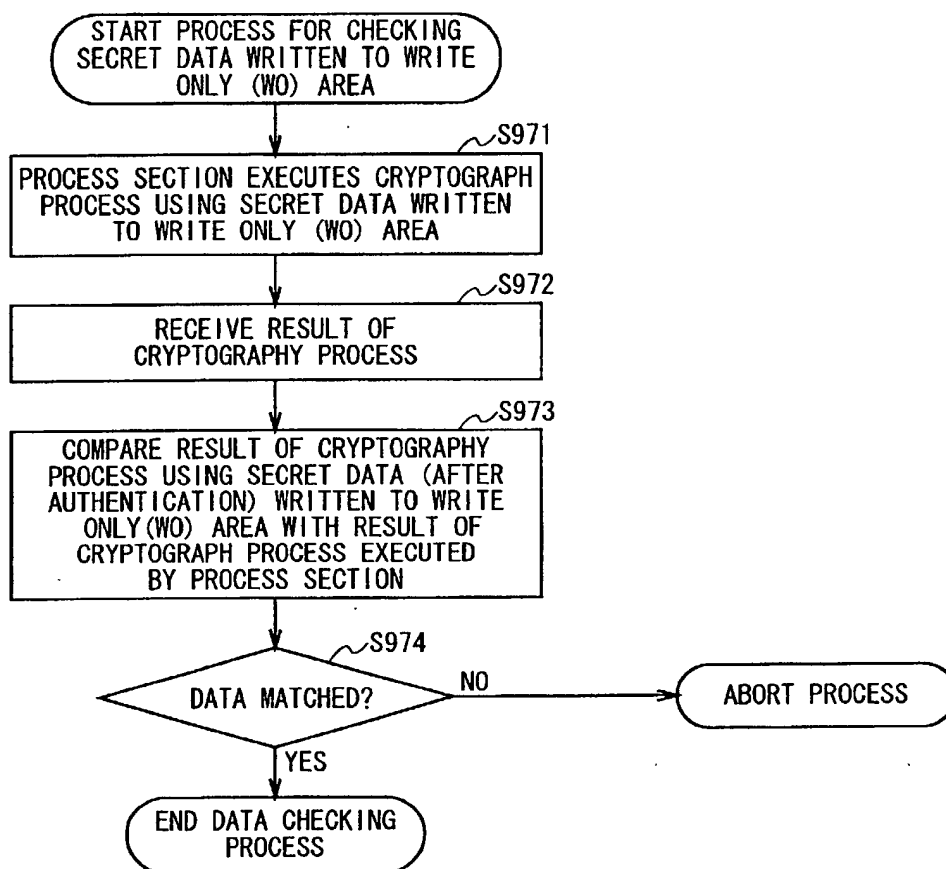


FIG. 93

## Explanation of Reference Numerals

106...main CPU, 107...RAM, 108...ROM, 109...AV process section,  
110...Input process section, 111...PIO, 112...SIO, 300...recording  
and reproducing device, 301...control section, 302...cryptography  
process section, 303...recording device controller, 304...read  
section, 305...communication section, 306...control section,  
307...internal memory, 308...encryption/decryption section,  
400...recording device, 401...cryptography process section,  
402...external memory, 403...control section, 404...communication  
section, 405...internal memory, 406...encryption/decryption  
section, 407...external memory control section, 500...medium, 600  
communication means, 2101, 2102, 2103...recording and reproducing  
device, 2104, 2105, 2106...recording device, 2901...command number  
managing section, 2902...command register, 2903,  
2904...authentication flag, 3001...speaker, 3002...monitor,  
3090...memory, 3091...content analysis section, 3092...data  
storage section, 3093...program storage section,  
3094...compression decompression process section, 7701...content  
data, 7702...revocation list, 7703...list check value,  
8000...security chip, 8001...process section, 8002...storage  
section, 8003...mode signal line, 8004...command signal line,  
8201...read write area, 8202...write only area.